XXIII

Appendix

Part XXIII: Contents

A Pedagogical comments and references

Here are some higher-level comments on the way specific topics were presented, as well as pointers to further reading.

§A.1 Basic algebra and topology

§A.1.i Linear algebra and multivariable calculus

Following the comments in Section 9.9, I dislike most presentations of linear algebra and multivariable calculus since they miss the two key ideas, namely:

- In linear algebra, we study *linear maps* between spaces.
- In calculus, we *approximate functions at points by linear functions.*

Thus, I believe linear algebra should *always* be taught before multivariable calculus. In particular, I do not recommend most linear algebra or multivariable calculus books.

For linear algebra, I've heard that [**Ax97**] follows this approach, hence the appropriate name "Linear Algebra Done Right". I followed with heavy modifications the proceedings of Math 55a, see [**Ga14**].

For multivariable calculus and differential geometry, I found the notes [**Sj05**] to be unusually well-written. I referred to it frequently while I was enrolled in Math 55b [**Ga15**].

§A.1.ii General topology

My personal view on spaces is that every space I ever work with is either metrizable or is the Zariski topology.

I adopted the approach of [**Pu02**], using metric topology first. I find that metric spaces are far more intuitive, and are a much better way to get a picture of what open / closed / compact etc. sets look like. This is the approach history took; general topology grew out of metric topology.

I personally dislike starting any general topology class by defining what a general topological space is, because it doesn't communicate a good picture of open and closed sets to draw pictures of.

§A.1.iii Groups and commutative algebra

I teach groups before commutative rings but might convert later. Rings have better examples, don't have the confusion of multiplicative notation for additive groups, and modding out by ideals is more intuitive.

There's a specific thing I have a qualm with in group theory: the way that the concept of a normal subgroup is introduced. Only [**Go11**] does something similar to what I do. Most other people simply *define* a normal subgroup N as one with gNg^{-1} and then proceed to define modding out, without taking the time to explain where this definition comes from. I remember distinctly this concept as the first time in learning math where I didn't understand what was going on. Only in hindsight do I see where this definition came from; I tried hard to make sure my own presentation didn't have this issue.

I deliberately don't include a chapter on just commutative algebra; other than the chapter on rings and ideals. The reason is that I always found it easier to learn commutative algebra theorems on the fly, in the context of something like algebraic number theory or algebraic geometry. For example, I finally understand why radicals and the Nullstellensatz were important when I saw how they were used in algebraic geometry. Before then, I never understood why I cared about them.

§A.1.iv Calculus

I do real analysis by using metric and general topology as the main ingredient, since I think it's the most useful later on and the most enlightening. In some senses, I am still following [Pu02].

§A.2 Second-year topics

§A.2.i Measure theory and probability

The main inspiration for these lectures is Vadim Gorin's 18.175 at MIT; [Go18] has really nice lecture notes taken by Tony Zhang. I go into a bit more details of the measure theory, and (for now) less into the probability. But I think probability is a great way to motivate measure theory anyways, and conversely, it's the right setting in to which state things like the central limit theorem.

I also found [Ch08] quite helpful, as another possible reference.

§A.2.ii Complex analysis

I picked the approach of presenting the Cauchy-Goursat theorem as given (rather than proving a weaker version by Stokes' theorem, or whatever), and then deriving the key result that holomorphic functions are analytic from it. I think this most closely mirrors the "real-life" use of complex analysis, i.e. the computation of contour integrals.

The main reference for this chapter was [Ya12], which I recommend.

§A.2.iii Category theory

I enthusiastically recommend [Le14], from which my chapters are based, and which contains much more than I had time to cover.

You might try reading chapters 2-4 in reverse order though: I found that limits were much more intuitive than adjoints. But your mileage may vary.

The category theory will make more sense as you learn more examples of structures: it will help to have read, say, the chapters on groups, rings, and modules.

§A.2.iv Quantum algorithms

The exposition given here is based off a full semester at MIT taught by Seth Lloyd, in 18.435J [Ll15]. It is written in a far more mathematical perspective.

I only deal with finite-dimensional Hilbert spaces, because that is all that is needed for Shor's algorithm, which is the point of this chapter. This is not an exposition intended for someone who wishes to seriously study quantum mechanics (though it might be a reasonable first read): the main purpose is to give students a little appreciation for what this "Shor's algorithm" that everyone keeps talking about is.

§A.2.v Representation theory

I staunchly support teaching the representation of algebras first, and then specializing to the case of groups by looking at $k[G]$. The primary influence for the chapters here is [Et11], and you might think of what I have here as just some selections from the first four chapters of this source.

§A.2.vi Set theory

Set theory is far off the beaten path. The notes I have written are based off the class I took at Harvard College, Math 145a [Ko14].

My general impression is that the way I present set theory (trying to remain intuitive and informal in a logical minefield) is not standard. Possible other reference: [Mi14].

§A.3 Advanced topics

§A.3.i Algebraic topology

I cover the fundamental group π_1 first, because I think the subject is more intuitive this way. A possible reference in this topic is [Mu00]. Only later do I do the much more involved homology groups. The famous standard reference for algebraic topology is [Ha02], which is what almost everyone uses these days. But I also found [Ma13a] to be very helpful, particularly in the part about cohomology rings.

I don't actually do very much algebraic topology. In particular, I think the main reason to learn algebraic topology is to see the construction of the homology and cohomology groups from the chain complex, and watch the long exact sequence in action. The concept of a (co)chain complex comes up often in other contexts as well, like the cohomology of sheaves or Galois cohomology. Algebraic topology is by far the most natural one.

I use category theory extensively, being a category-lover.

§A.3.ii Algebraic number theory

I learned from [Og10], using [Le02] for the part about the Chebotarev density theorem.

When possible I try to keep the algebraic number theory chapter close at heart to an "olympiad spirit". Factoring in rings like $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-5}]$ is very much an olympiad-flavored topic at heart: one is led naturally to the idea of factoring in general rings of integers, around which the presentation is built. As a reward for the entire buildup, the exposition finishes with the application of the Chebotarev density theorem to IMO 2003, Problem 6.

§A.3.iii Algebraic geometry

My preferred introduction to algebraic geometry is [Ga03] for a first read and [Va17] for the serious version. Both sets of lecture notes are essentially self-contained.

I would like to confess now that I know relatively little algebraic geometry, and in my personal opinion the parts on algebraic geometry are the weakest part of the Napkin. This is reflected in my work here: in the entire set of notes I only barely finish defining a scheme, the first central definition of the subject.

Nonetheless, I will foolishly still make some remarks about my own studies. I think there are three main approaches to beginning the study of schemes:

- Only looking at affine and projective varieties, as part of an "introductory" class, typically an undergraduate course.
- Studying affine and projective varieties closely and using them as the motivating example of a *scheme*, and then developing algebraic geometry from there.
- Jumping straight into the definition of a scheme, as in the well-respected and challenging [Va17].

I have gone with the second approach, I think that if you don't know what a scheme is, then you haven't learned algebraic geometry. But on the other hand I think the definition of a scheme is difficult to digest without having a good handle first on varieties.

These opinions are based on my personal experience of having tried to learn the subject through all three approaches over a period of a year. Your mileage may vary.

I made the decision to, at least for the second part, focus mostly on *affine* schemes. These already generalize varieties in several ways, and I think the jump is too much if one starts then gluing schemes together. I would rather that the student first feel like they really understand how an affine scheme works, before going on into the world where they now have a general scheme X which is locally affine (but probably not itself affine). The entire chapter dedicated to a gazillion examples of affine schemes is a hint of this.

§A.3.iv Riemann surfaces

My friend recommends [Mi95]. The preface of the book reads as follows:

> But I try to stress that the main examples (from the point of view of algebraic geometry) come from projective curves, and slowly but surely the text evolves to the algebraic category, culminating in an algebraic proof of the Riemann-Roch theorem. After returning to the analytic side of things for Abel's theorem, the progression is repeated again when sheaves and cohomology are discussed: first the analytic, then the algebraic category.

Thus you can also use this as a resource to learn algebraic geometry.

Occasionally, a few concepts are not very well-motivated, such as divisors, complex structure induced on plane curves, or line bundles. In these cases, we try to explain the motivation clearly in the Napkin.

§A.4 Topics not in Napkin

§A.4.i Analytic number theory

I never had time to write up notes in Napkin for these. If you're interested though, I recommend [Hi13]. They are highly accessible and delightful to read. The only real prerequisites are a good handle on Cauchy's residue formula.

B Hints to selected problems

1A. Orders.

1B. Copy the proof of Fermat's little theorem, using Lemma 1.2.5.

1C. For the former, decide where the isomorphism should send r and s, and the rest will follow through. For the latter, look at orders.

1D*. Generated groups.

1F†. Use $n = |G|$.

1G. For the lower bound, consider orders (note that 1009 is prime). For the upper bound, consider a 1009-gon.

1H. Draw inspiration from D_6.

1I. Look at the group of 2×2 matrices mod p with determinant ± 1.

2B. No. There is not even a continuous injective map from $\mathbb{Q}$ to $\mathbb{N}$.

2C. You can do this with bare hands. You can also use composition.

2D. $\pm x$ for good choices of $\pm$.

2E. Project gaps onto the y-axis. Use the fact that uncountably many positive reals cannot have finite sum.

2F. First answer the following question: "is $1/x$ a function?".

3A. Write it out: $\phi(ab) = \phi(a)\phi(b)$.

3B. Yes, no.

3C. No.

3D. $\gcd(1000, 999) = 1$.

3F. Find an example of order 8.

3G. Try to show G is the dihedral group of order 18. There is not much group theory content here — just manipulation.

3H. Get yourself a list of English homophones, I guess. Don't try too hard. Letter v is the worst; maybe $felt = veldt$?

4A. $R = \mathbb{R}[i]$.

4B. Show that the map

$$\begin{aligned} \mathbb{C}[x] &\to \mathbb{C} \times \mathbb{C} \\ p &\mapsto (p(0), p(1)) \end{aligned}$$

is surjective and calculate its kernel.

4E. For (b) homomorphism is uniquely determined by the choice of $\psi(x) \in R$

5A. Yes.

5B. The kernel is an ideal of K!

5C*. This is just a definition chase.

5D*. Fermat's little theorem type argument; cancellation holds in integral domains.

5E*. Just keep on adding in elements to get an ascending chain.

5F. Use the fact that both are PID's.

5G†. Show that the quotient $\mathbb{Z}[\sqrt{2017}]/I$ has finitely many elements for any nonzero prime ideal I. Therefore, the quotient is an integral domain, it is also a field, and thus I was a maximal ideal.

6A†. The main task is to show there exists some fixed point. Start at some point x_0 and consider the sequence $x_1 = T(x_0)$, $x_2 = T(x_1)$, $x_3 = T(x_2)$, …, and so on.

6B. (a): M is complete and bounded but not totally bounded. N is all no. For (b) show that $M \cong \mathbb{R} \cong N$.

6C†. As a set, we let $\overline{M}$ be the set of Cauchy sequences (x_n) in M, modulo the relation that $(x_n) \sim (y_n)$ if $\lim_n d(x_n, y_n) = 0$.

6E. The standard solution seems to be via the so-called "Baire category theorem".

7D. Let p be any point. If there is a real number r such that $d(p,q) \neq r$ for any $q \in M$, then the r-neighborhood of p is clopen.

7E. (a) is yes, and (b) is no even for metric spaces. In fact, a *totally disconnected* space is one for which every connected component consists of only a single point, and there are examples of totally disconnected metric spaces with non-discrete topologies.

7F. Note that $p\mathbb{Z}$ is closed for each p. If there were finitely many primes, then $\bigcup p\mathbb{Z} = \mathbb{Z} \setminus \{-1,1\}$ would have to be closed; i.e. $\{-1,1\}$ would be open, but all open sets here are infinite.

7G. The balls at 0 should be of the form $n! \cdot \mathbb{Z}$.

7H. Appeal to $\mathbb{Q}$.

8A. $[0,1]$ is compact.

8B. If and only if it is finite.

8E. Suppose $p_i = (x_i, y_i)$ is a sequence in $X \times Y$ $(i = 1, 2, \dots)$. Take a sub-sequence such that the x-coordinate converges (throwing out some terms). Then take a sub-sequence of *that* sub-sequence such that y-coordinate converges (throwing out more terms).

8F†. Mimic the proof of Theorem 8.2.2. The totally bounded condition lets you do Pigeonhole.

8H. Assuming M is not compact, construct an unbounded continuous function $F\colon M \to \mathbb{R}$. Once such a function F is defined, the metric

$$d'(x,y) := d(x,y) + |F(x) - F(y)|$$

will establish the contrapositive of the problem.

8I. The answer to both parts is no.

For (a) use Problem 8D.

For (b), color each circle in the partition based on whether it contains p but not q, q but not p, or both.

9A†. Use the rank-nullity theorem. Also consider the zero map.

9D. $a + b\sqrt{5} \mapsto \sqrt{5}a + 5b$.

9F. Plug in $y = -1, 0, 1$. Use dimensions of $\mathbb{R}[x]$.

9G. Interpret as $V \oplus V \to W$ for suitable V, W.

9I*. Use the fact that the infinite chain of subspaces

$$\ker T \subseteq \ker T^2 \subseteq \ker T^3 \subseteq \dots$$

and the similar chain for $\operatorname{im} T$ must eventually stabilize (for dimension reasons).

10D. The answer is yes. In fact, the result is true if $\mathbb{C}^{\oplus 2}$ is any finite-dimensional $\mathbb{C}$-vector space.

10F. Only 0 is. Look at degree.

10G. All of them are!

11A. Follows by writing T in an eigenbasis: then the diagonal entries are the eigenvalues.

11B†. Again one can just take a basis.

11C†. One solution is to just take a basis. Otherwise, interpret $T \otimes S \mapsto \operatorname{Tr}(T \circ S)$ as a linear map $(V^\vee \otimes W) \otimes (W^\vee \otimes V) \to k$, and verify that it is commutative.

11D. Look at the trace of T.

12A. The point is that

$$(v_1 + cv_2) \wedge v_2 \cdots \wedge v_n = v_1 \wedge v_2 \cdots \wedge v_n + c(v_2 \wedge v_2 \cdots \wedge v_n)$$

and the latter term is zero.

12B. You can either do this by writing T in matrix form, or you can use the wedge definition of $\det T$ with the basis given by Jordan form.

12C. This is actually immediate by taking any basis in which X is upper-triangular!

12D. You don't need eigenvalues (though they could work also). In one direction, recall that (by Problem 9B†) we can replace "isomorphism" by "injective". In the other, if T is an isomorphism, let S be the inverse map and look at $\det(S \circ T)$.

12E. Consider 1000×1000 matrix M with entries 0 on diagonal and ± 1 off-diagonal. Mod 2.

12F. There is a family of solutions other than just $a = b = c = d$.

One can solve the problem using Cayley-Hamilton. A more "bare-hands" approach is to show the matrix is invertible (unless $a = b = c = d$) and then diagonalize the matrix as $M = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ps\lambda_1 - qr\lambda_2 & qs(\lambda_1 - \lambda_2) \\ pr(\lambda_2 - \lambda_1) & ps\lambda_2 - qr\lambda_1 \end{bmatrix}$.

12G. Take bases, and do a fairly long calculation.

13B*. Fix an orthonormal basis $e_1, \dots, e_n$. Use the fact that $\mathbb{R}^n$ is complete.

13C. Dot products in $\mathbb{F}_2$.

13D*. Define it on simple tensors then extend linearly.

13E. $k = n^n$. Endow tensor products with an inner form. Note that "zero entry somewhere on its diagonal" is equivalent to the product of those entries being zero.

14A. Use Parseval again, but this time on $f(x) = x^2$.

14B. Define the Boolean function $D \colon \{\pm 1\}^3 \to \mathbb{R}$ by $D(a, b, c) = ab + bc + ca$. Write out the value of $D(a, b, c)$ for each (a, b, c). Then, evaluate its expected value.

15A*. You can *prove* the result just by taking a basis $e_1, \dots, e_n$ of V and showing that it is a linear map sending e_1 to the basis $(e_1^\vee)^\vee$.

15B. Use Theorem 9.7.6 and it will be immediate (the four quantities equal the k in the theorem).

15C†. This actually is just the previous problem in disguise! The row rank is $\dim \operatorname{im} T^\vee$ and the column rank is $\dim \operatorname{im} T$.

15F. If there is a polynomial, check $TT^\dagger = T^\dagger T$ directly. If T is normal, diagonalize it.

16A. Just apply Burnside's lemma directly to get the answer of 198 (the relevant group is D_{14}).

16B. There are multiple ways to see this. One is to just do the algebraic manipulation. Another is to use Cayley's theorem to embed G into a symmetric group.

16C. Double-count pairs (g, x) with $g \cdot x = x$.

16E†. Let G act on the left cosets $\{gH \mid g \in G\}$ by left multiplication: $g' \cdot gH = g'gH$. Consider the orbit $\mathcal{O}$ of the coset H. By the orbit-stabilizer theorem, $|\mathcal{O}|$ divides $|G|$. But $|\mathcal{O}| \le p$ also. So either $\mathcal{O} = \{H\}$ or $\mathcal{O}$ contains all cosets. The first case is impossible.

17B. Count Sylow 2 and 7 groups and let them intersect.

17C. Construct a non-abelian group such that all elements have order three.

17D. First, if G abelian it's trivial. Otherwise, let $Z(G)$ be the center of the group, which is always a normal subgroup of G. Do a mod p argument via conjugation (or use the class equation).

18A†. In the structure theorem, $k/(s_i) \in \{0, k\}$.

18B†. By theorem $V \cong \bigoplus_i k[x]/(s_i)$ for some polynomials s_i. Write each block in the form described.

18C†. Copy the previous proof, except using the other form of the structure theorem. Since $k[x]$ is algebraically closed each p_i is a linear factor.

18D. The structure theorem is an anti-result here: it more or less implies that finitely generated abelian groups won't work. So, look for an infinitely generated example.

18E. I think the result is true if you add the assumption A is Noetherian, so look for trouble by picking A not Noetherian.

19B†. For any $a \in A$, the map $v \mapsto a \cdot v$ is intertwining.

19C*. For part (b), pick a basis and do $T \mapsto (T(e_1), \dots, T(e_n))$.

19D*. Right multiplication.

19E. Apply Problem 9I*.

20A. They are all one-dimensional, n of them. What are the homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^\times$?

20B. The span of $(1, 0)$ is a subrepresentation.

20C. This is actually easy.

20D. There are only two one-dimensional ones (corresponding to the only two homomorphisms $D_{10} \to \mathbb{C}^\times$). So the remaining ones are two-dimensional.

20E. Let $r, t \in D_{10}$ be rotation and reflection respectively. Then we can sum over all possible bug's moves with

$$\frac{1}{10}\operatorname{Tr}(\rho(r) + \rho(t))^{15}.$$

Then use Problem 20D to compute this trace.

21A†. Obvious. Let $W = \bigoplus V_i^{m_i}$ (possible since $\mathbb{C}[G]$ semisimple) thus $\chi_W = \sum_i m_i \chi_{V_i}$.

21B. Use the previous problem, with $\chi_W = \chi_{\text{refl}_0}^2$.

21C. Characters. Note that $|\chi_W| = 1$ everywhere.

21D. There are five conjugacy classes, 1, -1 and $\pm i$, $\pm j$, $\pm k$. Given four of the representations, orthogonality can give you the fifth one.

21E*. Construct two square $r \times r$ matrices A and B such that AB is the identity by the first orthogonality. Then use BA to prove the second orthogonaliy relation.

23A. Rewrite $|\Psi_-\rangle = -\frac{1}{\sqrt{2}}\left(|{\to}\rangle_A \otimes |{\leftarrow}\rangle_B - |{\leftarrow}\rangle_A |{\to}\rangle_B\right)$.

23B. 1, 1, 1, -1 respectively. When we multiply them all together, we get that $\mathrm{id}^A \otimes \mathrm{id}^B \otimes \mathrm{id}^C$ has measurement -1, which is the paradox. What this means is that the values of the measurements can't be prepared in advance independently. In other words, this contradicts certain local hidden-variable theories.

This was one of several results for which Zeilinger won a (shared) Nobel Prize in 2022.

24A. One way is to create CCNOT using a few Fredkin gates.

24B. Plug in $|\psi\rangle = |0\rangle$, $|\psi\rangle = |1\rangle$, $|\psi\rangle = |{\to}\rangle$ and derive a contradiction.

24C. First show that the box sends $|x_1\rangle \otimes \cdots \otimes |x_m\rangle \otimes |{\leftarrow}\rangle$ to $(-1)^{f(x_1,\dots,x_m)}(|x_1\rangle \otimes \cdots \otimes |x_m\rangle \otimes |{\leftarrow}\rangle)$.

24D†. This is direct computation.

26B. Iff the sequence is convergent!

26D. The nth partial sum is $\frac{1}{1-r}(1-r^{n+1})$.

26F. This is a very tricky algebraic manipulation. Try setting $a_n = x_1 + \cdots + x_n$ for $x_i \ge 0$.

26G. This is trickier than it looks. We have $x_n = e^{x_n} - e^{x_{n+1}}$ but it requires some care to prove convergences. Helpful hint: $e^t \ge t+1$ for all real numbers t, therefore all x_n's are nonnegative.

26H. The limit always exists and equals zero. Consequently, f is continuous exactly at irrational points.

28G. First rewrite it as $f(x) = e^{x \log x}$.

29B†. Because you know all derivatives of sin and cos, you can compute their Taylor series, which converge everywhere on $\mathbb{R}$. At the same time, exp was defined as a Taylor series, so you can also compute it. Write them all out and compare.

29C†. Use repeated Rolle's theorem. You don't need any of the theory in this chapter to solve this, so it could have been stated much earlier; but then it would be quite unmotivated.

29D. Use Taylor's theorem.

30A. Contradiction and mean value theorem (again!).

30B*. For every positive integer n, take a partition where every rectangle has width $w = \frac{b-a}{n}$. Use the mean value theorem to construct a tagged partition such that the first rectangle has area $f(a+w) - f(a)$, the second rectangle has area $f(a+2w) - f(a+w)$, and so on; thus the total area is $f(b) - f(a)$.

30D. Write this as $\frac{1}{n}\sum_{k=1}^{n} \frac{1}{1+\frac{k}{n}}$. Then you can interpret it as a rectangle sum of a certain Riemann integral.

31A*. Look at the Taylor series of f, and use Cauchy's differentiation formula to show that each of the larger coefficients must be zero.

31B*. Proceed by contradiction, meaning there exists a sequence $z_1, z_2, \dots \to z$ where $0 = f(z_1) = f(z_2) = \dots$ all distinct. Prove that $f = 0$ on an open neighborhood of z by looking at the Taylor series of f and pulling out factors of z.

31C*. Take the interior of the agreeing points; show that this set is closed, which implies the conclusion.

31E. Liouville. Look at $\frac{1}{f(z)-w}$.

31F. You can adapt part of the proof of Cauchy-Goursat theorem presented above, and apply ML estimation lemma to prove $\oint_\gamma f(z)\,dz = 0$. In this case however, you already know f is holomorphic, so you must have $|\oint_{\gamma_i} f\,dz| \ge |\oint_\gamma f\,dz|$, without the $\frac{1}{4}$ factor.

32C. This is called a "wedge contour". Try to integrate over a wedge shape consisting of a sector of a circle of radius r, with central angle $\frac{2\pi}{n}$. Take the limit as $r \to \infty$ then.

32D. It's $\lim_{a\to\infty} \int_{-a}^{a} \frac{\cos x}{x^2+1}\,dx$. For each a, construct a semicircle.

36B. Show that

$$\mu^*(S) = \begin{cases} 0 & S = \varnothing \\ 1 & S \text{ bounded and nonempty} \\ \infty & S \text{ not bounded.} \end{cases}$$

This lets you solve (b) readily; I think the answer is just unbounded sets, $\varnothing$, and one-point sets.

39A. You can read it off Theorem 39.3.1.

39B. After Pontryagin duality, we need to show G compact implies $\widehat{G}$ discrete and G discrete implies $\widehat{G}$ compact. Both do not need anything fancy: they are topological facts.

41A. This is actually trickier than it appears, you cannot just push quantifiers (contrary to the name), but have to focus on $\varepsilon = 1/m$ for $m = 1, 2, \dots$.

The problem is saying for each $\varepsilon > 0$, if $n > N_\varepsilon$, we have $\mu(\omega : |X(\omega) - X_n(\omega)| \le \varepsilon) = 1$. For each m there are some measure zero "bad worlds"; take the union.

42B. There is a cute elementary solution. For the martingale-based solution, show that the fraction of red cards in the deck at time n is a martingale.

42E. Use Problem 42A.

42F. It occurs with probability 1. If X_n is the number on the board at step n, and $\mu = \frac{1}{2.01}\int_0^{2.01} \log t\,dt$, show that $\log(X_n) - n\mu$ is a martingale. (Incidentally, using the law of large numbers could work too.)

43B. Simply induct, with the work having been done on the $k = 2$ case.

44B. This is just a summation. You will need the fact that mixed partials are symmetric.

45A†. Direct application of Stokes' theorem to $\alpha = f\,dx + g\,dy$.

45B. This is just an exercises in sigma notation.

45D. This is a straightforward (but annoying) computation.

45E. We would want $\alpha_p(v) = \|v\|$.

45F. Show that $d^2 = 0$ implies $\int_{\partial c} \alpha = 0$ for exact α. Draw an annulus.

53B. Note that $p(x)$ is a minimal polynomial for r, but so is $q(x) = x^{\deg p} p(1/x)$. So q and p must be multiples of each other.

53C*. $\left|\frac{1}{n}(\varepsilon_1 + \dots + \varepsilon_n)\right| \le 1$.

53D†. Only the obvious ones. Assume $\cos(q\pi) \in \mathbb{Q}$. Let ζ be a root of unity (algebraic integer as $\zeta^N - 1 = 0$ for some N) and note that $2\cos(q\pi) = \zeta + \zeta^{N-1}$ is both an algebraic integer and a rational number.

53E. View as roots of unity. Note $\frac{1}{2}$ isn't an algebraic integer.

53F. Let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be its conjugates. Look at the polynomial $(x-\alpha_1^e)\dots(x-\alpha_n^e)$ across $e \in \mathbb{N}$. Pigeonhole principle on all possible polynomials.

54A*. The norm is multiplicative and equal to product of Galois conjugates.

54B*. It's isomorphic to K.

54C. Taking the standard norm on $\mathbb{Q}(\sqrt{2})$ will destroy it.

54D. Norm in $\mathbb{Q}(\sqrt[3]{2})$.

54E†. Obviously $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K$, so our goal is to show the reverse inclusion. Show that for any $\alpha \in \mathcal{O}_K$, the trace of $\alpha(1-\zeta_p)$ is divisible by p. Given $x = a_0 + a_1\zeta_p + \dots + a_{p-2}\zeta^{p-2} \in \mathcal{O}_K$ (where $a_i \in \mathbb{Q}$), consider $(1-\zeta_p)x$.

55C. Copy the proof of the usual Fermat's little theorem.

55D†. Clear denominators!

55E. (a) is straightforward. For (b) work mod p. For (c) use norms.

56A. Repeat the previous procedure.

56B. You should get a group of order three.

56C. Mimic the proof of part (a) of Minkowski's theorem.

56D. Linear algebra.

56E. Factor in $\mathbb{Q}(i)$.

56F. Factor p, show that the class group of $\mathbb{Q}(\sqrt{-5})$ has order two.

57A*. Direct linear algebra computation.

57B*. Let M be the "embedding" matrix. Look at $M^\top M$, where $M^\top$ is the transpose matrix.

57C*. Vandermonde matrices.

57D. $M_K \ge 1$ must hold. Bash.

59A*. Look at the image of ζ_p.

59C. Repeated quadratic extensions have degree 2, so one can only get powers of two.

59E. Hint: $\sigma(x^2) = \sigma(x)^2 \ge 0$ plus Cauchy's Functional Equation.

59F. By induction, suffices to show $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ for some γ in terms of α and β. For all but finitely many rational λ, the choice $\gamma = \alpha + \lambda\beta$ will work.

60A†. The Fibonacci sequence is given by $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the two roots of $P(X) \overset{\text{def}}{=} X^2 - X - 1$. Show the polynomial $P(X)$ is irreducible modulo 127; then work in the splitting field of P, namely $\mathbb{F}_{p^2}$.

Show that $\mathbb{F}_p = -1$, $\mathbb{F}_{p+1} = 0$, $\mathbb{F}_{2p+1} = 1$, $\mathbb{F}_{2p+2} = 0$. (Look at the action of $\operatorname{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ on the roots of P.)

61A†. Show that no rational prime p can remain inert if $\operatorname{Gal}(K/\mathbb{Q})$ is not cyclic. Indeed, if p is inert then $D_p \cong \operatorname{Gal}(K/\mathbb{Q})$.

62A. Modify the end of the proof of quadratic reciprocity.

62C†. Chebotarev Density on $\mathbb{Q}(\zeta_m)$.

62E. By primitive roots, it's the same as the action of ×3 on $\mathbb{Z}/(p-1)\mathbb{Z}$. Let ζ be a $(p-1)$st root of unity. Take $d = \prod_{i<j}(\zeta^i - \zeta^j)$, think about $\mathbb{Q}(d)$, and figure out how to act on it by $x \mapsto x^3$.

63A†. Pick m so that $\mathfrak{f}(L/\mathbb{Q}) \mid m\infty$.

63B†. Apply the Takagi existence theorem with $\mathfrak{m} = 1$.

63C. The extension $L/\mathbb{Q}$ is not abelian.

64C†. Prove and use the fact that a quotients of compact spaces remain compact.

68A. The category $\mathcal{A} \times \mathbf{2}$ has "redundant arrows".

71A. Take the $n-1$st homology groups.

71B. Build F as follows: draw the ray from x through $f(x)$ and intersect it with the boundary S^{n-1}.

72A. Induction on m, using hemispheres.

72B. One strategy is induction on p, with base case $p = 1$. Another strategy is to let U be the desired space and let V be the union of p non intersecting balls.

72C*. Use Theorem 72.2.5. Note that $\mathbb{R}^n \setminus \{0\}$ is homotopy equivalent to S^{n-1}.

72D. $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ is a short exact sequence of chain complexes. Write out the corresponding long exact sequence. Nearly all terms will vanish.

72E*. It's possible to use two cylinders with U and V. This time the matrix is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ or some variant though; in particular, it's injective, so $\widetilde{H}_2(X) = 0$.

72F*. Find a new short exact sequence to apply Theorem 72.2.1 to.

73B. Use Theorem 72.2.5.

73E. For any n, prove by induction for $k = 1, \dots, n-1$ that (a) if X is a subset of S^n homeomorphic to D^k then $\widetilde{H}_i(S^n \setminus X) = 0$; (b) if X is a subset of S^n homeomorphic to S^k then $\widetilde{H}_i(S^n \setminus X) = \mathbb{Z}$ for $i = n-k-1$ and 0 otherwise.

74A†. $\mathbb{CP}^n$ has no cells in adjacent dimensions, so all d_k maps must be zero.

74B. The space $S^n - \{x_0\}$ is contractible.

74D. You won't need to refer to any elements. Start with

$$H_2(X) \cong H_2(X^3) \cong H_2(X^2)/\ker\left[H_2(X^2) \twoheadrightarrow H_2(X^3)\right],$$

say. Take note of the marked injective and surjective arrows.

74E†. There is one cell of each dimension. Show that the degree of d_k is $\deg(\mathrm{id})+\deg(-\mathrm{id})$, hence d_k is zero or $\cdot 2$ depending on whether k is even or odd.

76A†. Write $H^k(M;\mathbb{Z})$ in terms of $H_k(M)$ using the UCT, and analyze the ranks.

76B. Use the previous result on Betti numbers.

76C. Use the $\mathbb{Z}/2\mathbb{Z}$ cohomologies, and find the cup product.

76D. Assume that $r\colon S^m \times S^n \to S^m \vee S^n$ is such a map. Show that the induced map $H^\bullet(S^m \vee S^n;\mathbb{Z}) \to H^\bullet(S^m \times S^n;\mathbb{Z})$ between their cohomology rings is monic (since there exists an inverse map i).

77B. Squares are nonnegative.

77C. This is actually an equivalent formulation of the Weak Nullstellensatz.

77D. Use the weak Nullstellensatz on $n+1$ dimensions. Given f vanishing on everything, consider $x_{n+1}f - 1$.

80B. You will need to know about complex numbers in Euclidean geometry to solve this problem.

81B†. Use the standard affine charts.

81C. Examine the global regular functions.

81D. Assume f was an isomorphism. Then it gives an isomorphism $f^\sharp\colon \mathcal{O}_V(V) \to \mathcal{O}_X(X) = \mathbb{C}[x,y]$. Thus we may write $\mathcal{O}_V(V) = \mathbb{C}[a,b]$, where $f^\sharp(a) = x$ and $f^\sharp(b) = y$. Let $f(p) = q$ where $\mathcal{V}(a,b) = \{q\}$. Use the definition of pullback to prove $p \in \mathcal{V}(x,y)$, contradiction.

82C. The stalk is R at points in the closure of $\{p\}$, and 0 elsewhere.

82D. Show that the complement $\{p \mid [s]_p = 0\}$ is open.

83B. Consider zero divisors.

83C*. Only one! A proof will be given a few chapters later.

83D. No. Imagine two axes.

84A. Galois conjugates.

85B. $k[x,y] \times k[z,z^{-1}]$.

85D. It's isomorphic to R!

87A. Use the fact that $\mathsf{AffSch} \simeq \mathsf{CRing}$.

88A. Let $\varepsilon = \pi - 3.141592653 < 10^{-9}$. Find $f(\varepsilon)$.

89E. This is an application of Axiom of Choice.

91A. $\sup_{k\in\omega} |V_k|$.

91B. Rearrange the cofinal maps to be nondecreasing.

92C†. This is very similar to the proof of Löwenheim-Skolem. For a sentence ϕ, let f_ϕ send α to the least $\beta < \kappa$ such that for all $\vec{b} \in V_\alpha$, if there exists $a \in M$ such that $V_\kappa \vDash \phi[a, \vec{b}]$ then $\exists a \in V_\beta$ such that $V_\kappa \vDash \phi[a, \vec{b}]$. (To prove this β exists, use the fact that κ is cofinal.) Then, take the supremum over the countably many sentences for each α.

92D*. Use Lemma 92.5.1. To prove $V_\kappa \vDash$ PowerSet you need κ to be a strong limit cardinal, and to prove $V_\kappa \vDash$ Replacement you need κ to be inaccessible — this is why we cared about cofinality and inaccessibility.

93B. Let D_1, D_2, ... be the dense sets (there are countably many of them).

94A. Assume not, and take $\lambda > \kappa$ regular in M; if $f \colon \overline{\lambda} \to \lambda$, use the Possible Values Argument on f to generate a function in M that breaks cofinality of λ.

C Sketches of selected solutions

1A. The point is that $\heartsuit$ is a group, $G \subsetneq \heartsuit$ a subgroup and $G \cong \heartsuit$. This can only occur if $|\heartsuit| = \infty$; otherwise, a proper subgroup would have strictly smaller size than the original.

1B. Let $\{g_1, g_2, \dots, g_n\}$ denote the elements of G. For any $g \in G$, this is the same as the set $\{gg_1, \dots, gg_n\}$. Taking the entire product and exploiting commutativity gives $g^n \cdot g_1 g_2 \dots g_n = g_1 g_2 \dots g_n$, hence $g^n = 1$.

1C. One can check manually that $D_6 \cong S_3$, using the map $r \mapsto (1\ 2\ 3)$ and $s \mapsto (1\ 2)$. (The right-hand sides are in "cycle notation", as mentioned in Section 6.iv.) On the other hand D_{24} contains an element of order 12 while S_4 does not.

1D*. Let G be a group of order p, and $1 \neq g \in G$. Look at the group H generated by g and use Lagrange's theorem.

1F†. The idea is that each element $g \in G$ can be thought of as a permutation $G \to G$ by $x \mapsto gx$.

1G. The answer is $n = 1009$. This solution uses the fact that 1009 is prime.

To show that no smaller m is possible, note that D_{2018} has elements of order 1009, a prime. Since S_n has no elements of this order for $n < 1009$, we need $n \geq 1009$.

To give a construction from $n = 1009$, note that D_{2018} can be thought of the symmetries of a 1009-gon. If one labels the vertices of the 1009-gon by $S := \{1, 2, \dots, 1009\}$, then elements of D_{2018} induces permutations on S, and the set of permutations achieved is the desired subgroup.

1H. We have $www = bb$, $bww = wb$, $wwb = bw$, $bwb = ww$. Interpret these as elements of D_6.

1I. Look at the group G of 2×2 matrices mod p with determinant ± 1 (whose entries are the integers mod p). Let $g = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and then use $g^{|G|} = 1_G$.

2B. Two possible approaches, one using metric definition and one using open sets.

Metric approach: I claim there is no injective map from $\mathbb{Q}$ to $\mathbb{N}$ that is continuous. Indeed, suppose f was such a map and $f(x) = n$. Then, choose $\varepsilon = 1/2$. There should be a $\delta > 0$ such that everything with δ of x in $\mathbb{Q}$ should land within ε of $n \in \mathbb{N}$ — i.e., is equal to n. This is a blatant contradiction of injectivity.

Open set approach: In $\mathbb{Q}$, no singleton set is open, whereas in $\mathbb{N}$, they all are (in fact $\mathbb{N}$ is discrete). As you'll see at the start of Chapter 7, with the new and improved definition of "homeomorphism", we found out that the structure of open sets on $\mathbb{Q}$ and $\mathbb{N}$ are different, so they are not homeomorphic.

2C. For subtraction, the map $x \mapsto -x$ is continuous so you can view it as a composed map

$$\begin{tikzcd}
\mathbb{R} \times \mathbb{R} \arrow[r, "(\mathrm{id},-x)"] & \mathbb{R} \times \mathbb{R} \arrow[r, "+"] & \mathbb{R} \\
(a,b) \arrow[r, mapsto] & (a,-b) \arrow[r, mapsto] & a-b.
\end{tikzcd}$$

Similarly, if you are willing to believe $x \mapsto 1/x$ is a continuous function, then division is composition

$$\begin{tikzcd}
\mathbb{R} \times \mathbb{R}_{>0} \arrow[r, "(\mathrm{id},1/x)"] & \mathbb{R} \times \mathbb{R}_{>0} \arrow[r, "\times"] & \mathbb{R} \\
(a,b) \arrow[r, mapsto] & (a,1/b) \arrow[r, mapsto] & a/b.
\end{tikzcd}$$

If for some reason you are suspicious that $x \mapsto 1/x$ is continuous, then here is a proof using sequential continuity. Suppose $x_n \to x$ with $x_n > 0$ and $x > 0$ (since x needs to be in $\mathbb{R}_{>0}$ too). Then

$$\left| \frac{1}{x} - \frac{1}{x_n} \right| = \frac{|x_n - x|}{|x x_n|}.$$

If n is large enough, then $|x_n| > x/2$; so the denominator is at least $x^2/2$, and hence the whole fraction is at most $\frac{2}{x^2}\left|x_n - x\right|$, which tends to zero as $n \to \infty$.

2D. Let $f(x) = x$ for $x \in \mathbb{Q}$ and $f(x) = -x$ for irrational x.

2E. Assume for contradiction it is completely discontinuous; by scaling set $f(0) = 0$, $f(1) = 1$ and focus just on $f \colon [0,1] \to [0,1]$. Since it's discontinuous everywhere, for every $x \in [0,1]$ there's an $\varepsilon_x > 0$ such that the continuity condition fails. Since the function is strictly increasing, that can only happen if the function misses all y-values in the interval $(f(x) - \varepsilon_x, f(x))$ or $(f(x), f(x) + \varepsilon_x)$ (or both).

Projecting these missing intervals to the y-axis you find uncountably many intervals (one for each $x \in [0,1]$) all of which are disjoint. In particular, summing the ε_x you get that a sum of uncountably many positive reals is 1.

But in general it isn't possible for an uncountable family $\mathcal{F}$ of positive reals to have finite sum. Indeed, just classify the reals into buckets $\frac{1}{k} \le x < \frac{1}{k-1}$. If the sum is actually finite then each bucket is finite, so the collection $\mathcal{F}$ must be countable, contradiction.

2F. Like most Internet "debates" about math, the question revolves around sloppy definitions. The original posed question (which is ill-formed) is

(1) Is $1/x$ a continuous function?

To make it well-formed, I want to *first* bring up the question:

(2) Is $1/x$ a function?

Technically, this question is *also* ill-formed because it never specifies the domain of the function, which is part of the data needed to specify a function. One reasonable guess what the asker meant would be $\mathbb{R} \setminus \{0\}$, i.e. the set of nonzero real numbers, in which case we get the question

(2') Does $1/x$ define a function from $\mathbb{R} \setminus \{0\}$ to $\mathbb{R}$?

which has the firm answer YES.

On the other hand, it does *not* make sense to try to define $1/x$ as a function on $\mathbb{R}$. The definition a function requires you to specify an output value for every input, so at least if you want a real-valued function[1], there isn't any way to construe $1/x$ as a function on all of $\mathbb{R}$.

Now, returning to (1), we can now ask a well-formed question

(1') Does $1/x$ describe a continuous function from $\mathbb{R} \setminus \{0\} \to \mathbb{R}$?

which again has the firm answer YES.

Of course, you could also consider a question like "does $1/x$ describe a continuous function $\mathbb{R} \to \mathbb{R}$?". However, this feels misleading: it would be like asking "is $\sqrt{2}$ an even integer?". The question doesn't make sense to begin with because $\sqrt{2}$ isn't an integer, and "even" is an adjective used for integers, so trying to ask whether it applies to $\sqrt{2}$ is a type-error. Similarly, "continuous" is an adjective used for functions; it doesn't make sense to ask whether it applies to something that isn't a function.

See `https://twitter.com/davidcpvm/status/1481024944830046209` for the Twitter post (in Spanish) and the accompanying Reddit post (one of several) at `https://www.reddit.com/r/math/comments/s82vf8`.

3A. Abelian groups: $abab = a^2b^2 \iff ab = ba$.

3B. Yes to (a): you can check this directly from the ghg^{-1} definition. For example, for (a) it is enough to compute $(r^a s)r^n(r^a s)^{-1} = r^{-n} \in H$. The quotient group is $\mathbb{Z}/2\mathbb{Z}$.

The answer is no for (b) by following Example 3.5.2.

3C. A subgroup of order 3 must be generated by an element of order 3, since 3 is prime. So we may assume WLOG that $H = \langle (1\ 2\ 3) \rangle$ (by renaming elements appropriately). But then let $g = (3\ 4)$; one can check $gHg^{-1} \neq H$.

3D. $G/\ker G$ is isomorphic to a subgroup of H. The order of the former divides 1000; the order of the latter divides 999. This can only occur if $G/\ker G = \{1\}$ so $\ker G = G$.

3F. Quaternion group.

3G. The answer is $|G| = 18$.

First, observe that by induction we have

$$a^n c = ca^{8n}$$

for all $n \geq 1$. We then note that

$$\begin{aligned} a(bc) &= (ab)c \\ a \cdot ca^6 &= c^2a^4 \cdot c \\ ca^8 \cdot a^6 &= c^2a^4 \cdot c \\ a^{14} &= c(a^4c) = c^2a^{32}. \end{aligned}$$

[1] Those of you that know what $\mathbb{RP}^1$ is could consider it as a function $\mathbb{RP}^1 \to \mathbb{RP}^1$ if you insisted; but it's continuous in that case too.

Hence we conclude $c^2 = a^{-18}$. Then $ab = c^2a^4 \implies b = a^{-15}$.

In that case, if $c^{2018} = b^{2019}$, we conclude $1 = a^{2018\cdot 18 - 2019\cdot 15} = a^{6039}$. Finally,

$$\begin{aligned} bc &= ca^6 \\ a^{-15}c &= ca^6 \\ a^{-15}c^2 &= c(a^6c) = c^2a^{48} \\ a^{-33} &= a^{30} \\ \implies a^{63} &= 1. \end{aligned}$$

Since $\gcd(6039, 63) = 9$, we find $a^9 = 1$, hence finally $c^2 = 1$. So the presentation above simplifies to

$$G = \left\langle a, c \mid a^9 = c^2 = 1,\ ac = ca^{-1} \right\rangle$$

which is the presentation of the dihedral group of order 18. This completes the proof.

3H. You can find many solutions by searching "homophone group"; one is `https://math.stackexchange.com/q/843966/229197`.

4A. This is just $\mathbb{R}[i] = \mathbb{C}$. The isomorphism is given by $x \mapsto i$, which has kernel (x^2+1).

4B. Note that the map

$$\begin{aligned} \mathbb{C}[x] &\to \mathbb{C} \times \mathbb{C} \\ p &\mapsto (p(0), p(1)) \end{aligned}$$

is indeed a surjective ring homomorphism. Its kernel consists of those polynomials p such that $p(0) = p(1) = 0$; this is the set of polynomials divisible by both x and $x-1$, so it is $x(x-1)$.

5C*. Consider $ab \in \phi^{\text{pre}}(I)$, meaning $\phi(ab) = \phi(a)\phi(b) \in I$. Since I is prime, either $\phi(a) \in I$ or $\phi(b) \in I$. In the former case we get $a \in \phi^{\text{pre}}(I)$ as needed; the latter case we get $b \in \phi^{\text{pre}}(I)$.

5D*. Let $x \in R$ with $x \neq 0$. Look at the powers x, x^2, ... By pigeonhole, eventually two of them coincide. So assume $x^m = x^n$ where $m < n$, or equivalently

$$0 = x \cdot x \cdot \dots \cdot x \cdot \left(x^{n-m} - 1\right).$$

Since $x \neq 0$, we get $x^{n-m} - 1 = 0$, or $x^{n-m} = 1$. So x^{n-m-1} is an inverse for x.

This means every nonzero element has an inverse, ergo R is a field.

5E*. For part (b), look at the poset of *proper* ideals. Apply Zorn's lemma (again using a union trick to verify the condition; be sure to verify that the union is proper!). In part (a) we are given no ascending infinite chains, so no need to use Zorn's lemma.

5F. The ideal (0) is of course prime in both. Also, both rings are PID's.

For $\mathbb{C}[x]$ we get a prime ideal $(x-z)$ for each $z \in \mathbb{C}$.

For $\mathbb{R}[x]$ a prime ideal $(x-a)$ for each $a \in \mathbb{R}$ and a prime ideal $(x^2 - ax + b)$ for each quadratic with two conjugate non-real roots.

5G†. Only one; the ideal (0) which is not maximal. We contend every other prime ideal is maximal.

Indeed, let I be any ideal (not necessarily prime), and let $a + b\sqrt{2017}$ be a nonzero element of it. Then I also contains $(a^2 - 2017b^2)$. That means when taking modulo I we may take modulo the integer $n := |a^2 - 2017b^2| \neq 0$.

So every element in R is equivalent modulo I to an element of the form $x + y\sqrt{2017}$, where $x, y \in \{0, 1, \dots, n-1\}$. In other words, the quotient R/I has at most finitely many elements.

When I is prime, it follows R/I is an integral domain, too. An integral domain with finitely many elements must be a field. Hence, from R/I being a field, we conclude I is maximal.

5H. The ideals are (0), $(1) = R$, and $(5^n) = 5^n R$ for each $n \geq 1$. The ideal (0) is prime and the ideal (5) is maximal (because the quotient $R/(5) \cong \mathbb{F}_5$ is a field).

6A†. Uniqueness of the fixed point follows from noting that if $T(p) = p$ and $T(q) = q$ and $p \neq q$ then we get a direct contradiction by plugging this into the given statement. Hence the main task is to show there exists some fixed point.

Start with any point x_0. Let $x_1 = T(x_0)$, $x_2 = T(x_1)$, $x_3 = T(x_2)$, …, and so on. We contend that $(x_0, x_1, x_2, \dots)$ is a Cauchy sequence. Indeed, if we let $r := 0.999 < 1$ and $c := d(x_0, x_1)$, then

$$\begin{aligned} d(x_1, x_2) &< r \cdot c \\ d(x_2, x_3) &< r^2 \cdot c \\ d(x_3, x_4) &< r^3 \cdot c \\ &\vdots \end{aligned}$$

and so for large $M < N$ we have

$$d(x_M, x_N) < \left(r^M + r^{M+1} + \dots + r^N\right) \cdot c < \frac{r^M}{1-r} \cdot c$$

which tends to zero once M is large enough.

Hence, because M is complete, the sequence must converge to some limit x. Because T is continuous, we get

$$T(x) = T\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} T(x_n) == \lim_{n\to\infty} x_{n+1} = x$$

as desired.

6B. Part (a) is essentially by definition. The space M is bounded since no distances exceed 1, but not totally bounded since we can't cover M with finitely many $\frac{1}{2}$-neighborhoods. The space M is complete since a sequence of real numbers converges in M if it converges in the usual sense. As for N, the sequence -1, -2, … is Cauchy but fails to converge; and it is obviously not bounded.

To show (b), the identity map (!) is an homeomorphism $M \cong \mathbb{R}$ and $\mathbb{R} \cong N$, since it is continuous.

This illustrates that $M \cong N$ despite the fact that M is both complete and bounded but N is neither complete nor bounded. On the other hand, we will later see that complete and totally bounded implies *compact*, which is a very strong property preserved under homeomorphism.

6D. See https://math.stackexchange.com/q/556150/229197.

7E. Part (a) is straightforward: assume for contradiction that the connected component of p is a disjoint union $U \sqcup V$ of two nonempty sets open in X. WLOG, assume $x \in U$ Let S be one of the subspaces containing X that intersects V. Then $S = (S \cap U) \sqcup (S \cap V)$ rewrites S as the disjoint union of two sets which are open in S, contradicting the connectedness of S.

(Though note that as S is not necessarily open in X, the sets $S \cap U$ and $S \cap V$ are not necessarily open in X either.)

For (b), a counterexample is to take any *totally disconnected* space like the Cantor set or the p-adic numbers.

7G. Let $d(x, y) = 2017^{-n}$, where n is the largest integer such that $n!$ divides $|x - y|$.

7H. You can pick a rational number in each interval and there are only countably many rational numbers. Done!

8A. Compactness is preserved under homeomorphism, but $[0, 1]$ is compact while $(0, 1)$ is not.

8E. Suppose $p_i = (x_i, y_i)$ is a sequence in $X \times Y$ ($i = 1, 2, \dots$). Looking on the X side, some subsequence converges: for the sake of illustration say it's $x_1, x_4, x_9, x_{16}, \dots \to x$. Then look at the corresponding sequence $y_1, y_4, y_9, y_{16}, \dots$. Using compactness of Y, it has a convergent subsequence, say $y_1, y_{16}, y_{81}, y_{256}, \dots \to y$. Then $p_1, p_{16}, p_{81}, \dots$ will converge to (x, y).

One common mistake is to just conclude that (x_n) has a convergent subsequence and that (y_n) does too. But these sequences could be totally unrelated. For this proof to work, you do need to apply compactness of X first, and then compactness of Y on the resulting *filtered* sequence like we did here.

8H. The following solution is due to Royce Yao. We show the contrapositive: if M is not compact, then there exists a homeomorphic unbounded metric.

The main step is to construction an unbounded continuous function $F \colon M \to \mathbb{R}$. Once such a function F is defined, the metric

$$d'(x, y) := d(x, y) + |F(x) - F(y)|$$

will solve the problem.

So, let a_1, a_2, … be a sequence in M with no convergent subsequence. For each a_i, there exists a radius r_i such that

$$0 < r_i < \frac{1}{2} \min_j d(a_i, a_j)$$

Define C_i as an open ball at a_i with radius r_i. Note that every ball is disjoint. Then, we define F as follow

$$F(x) = \begin{cases} 0 & x \notin C_i \\ \frac{i}{r_1}(r_i - d(x, a_i)) & x \in C_i \end{cases}$$

which can be seen to be continuous. Then, F is unbounded by considering $F(a_i)$ as i goes to infinity.

8I. Part (a) follows by the Cantor intersection theorem (Problem 8D). Assume for contradiction such a partition existed. Take any of the circles C_0, and let K_0 denote the closed disk with boundary C_0. Now take the circle C_1 passing through the center of C_0, and let K_1 denote the closed disk with boundary C_1. If we repeat in this way, we get a nested sequence $K_0 \supseteq K_1 \supseteq \dots$ and the radii of C_i approach zero (since each is at most half the previous once). Thus some point p lies in $\bigcap_n K_n$ which is impossible.

Now for part (b), again assume for contradiction a partition into circles exists. Color a circle magenta if it contains p but not q and color a circle cyan if it contains q but not p. Color p itself magenta and q itself cyan as well. Finally, color a circle neon yellow if it contains both p and q. (When we refer to coloring a circle, we mean to color all the points on it.)

By repeating the argument in (a) there are no circles enclosing neither p nor q. Hence every point is either magenta, cyan, or neon yellow. Now note that given any magenta circle, its interior is completely magenta. Actually, the magenta circles can be totally ordered by inclusion (since they can't intersect). So we consider two cases:

- If there is a magenta circle which is maximal by inclusion (i.e. a magenta circle not contained in any other magenta circle) then the set of all magenta points is just a closed disk.
- If there is no such magenta circle, then the set of magenta points can also be expressed as the union over all magenta circles of their interiors. This is a union of open sets, so it is itself open.

We conclude the set of magenta points is either a closed disk or an open set. Similarly for the set of cyan points. Moreover, the set of such points is convex.

To finish the problem:

- Suppose there are no neon yellow points. If the magenta points form a closed disk, then the cyan points are $\mathbb{R}^2$ minus a disk which is not convex. Contradiction. So the magenta points must be open. Similarly the cyan points must be open. But $\mathbb{R}^2$ is connected, so it can't be written as the union of two open sets.
- Now suppose there are neon yellow points. We claim there is a neon yellow circle minimal by inclusion. If not, then repeat the argument of (a) to get a contradiction, since any neon yellow circle must have diameter the distance from p to q. So we can find a neon yellow circle $\mathscr{C}$ whose interior is all magenta and cyan. Now repeat the argument of the previous part, replacing $\mathbb{R}^2$ by the interior of $\mathscr{C}$.

9A†.

	T injective	T surjective	T isomorphism
If $\dim V > \dim W \dots$	never	sometimes	never
If $\dim V = \dim W \dots$	sometimes	sometimes	sometimes
If $\dim V < \dim W \dots$	sometimes	never	never

Each "never" is by the rank-nullity theorem. Each counterexample is obtained by the zero map sending every element of V to zero; this map is certainly neither injective or surjective.

9B†. It essentially follows by Theorem 9.7.6.

9D. Since $1 \mapsto \sqrt{5}$ and $\sqrt{5} \mapsto 5$, the matrix is $\begin{bmatrix} 0 & 5 \\ 1 & 0 \end{bmatrix}$.

9G. Let V be the space of real polynomials with degree at most $d/2$ (which has dimension $1 + \lfloor d/2 \rfloor$), and W be the space of real polynomials modulo P (which has dimension d). Then $\dim(V \oplus V) > \dim W$. So the linear map $V \oplus V \to W$ by $(A, B) \mapsto A + Q \cdot B$ has a kernel of positive dimension (by rank-nullity, for example).

9I*. Consider

$$\{0\} \subsetneq \ker S \subseteq \ker S^2 \subseteq \ker S^3 \subseteq \dots \text{ and } V \supsetneq \operatorname{im} S \supseteq \operatorname{im} S^2 \supseteq \operatorname{im} S^3 \supseteq \dots.$$

For dimension reasons, these subspaces must eventually stabilize: for some large integer N, $\ker T^N = \ker T^{N+1} = \dots$ and $\operatorname{im} T^N = \operatorname{im} T^{N+1} = \operatorname{im} T^{N+2} = \dots$. When this happens, $\ker T^N \bigcap \operatorname{im} T^N = \{0\}$, since T^N is an automorphism of $\operatorname{im} T^N$. On the other hand, by Rank-Nullity we also have $\dim \ker T^N + \dim \operatorname{im} T^n = \dim V$. Thus for dimension reasons, $V = \ker T^N \oplus \operatorname{im} T^N$.

10A. It's just $\dim V = 2018$. After all, you are adding the dimensions of the Jordan blocks...

10B. (a): if you express T as a matrix in such a basis, one gets a diagonal matrix. (b): this is just saying each Jordan block has dimension 1, which is what we wanted. (We are implicitly using uniqueness of Jordan form here.)

10C. The $+1$ eigenspace is spanned by $e_1 + e_2$. The -1 eigenspace is spanned by $e_1 - e_2$.

10E. The $+1$ eigenspace is spanned by $1 + x^2$ and x. The -1 eigenspace is spanned by $1 - x^2$.

10F. Constant functions differentiate to zero, and these are the only 0-eigenvectors. There can be no other eigenvectors, since if $\deg p > 0$ then $\deg p' = \deg p - 1$, so if p' is a constant real multiple of p we must have $p' = 0$, ergo p is constant.

10G. e^{cx} is an example of a c-eigenvector for every c. If you know differential equations, these generate all examples!

11A. We saw already the trace is always the sum of the eigenvalues, in *any* basis. In particular, choosing the Jordan form basis from the previous chapter gives the result because the Jordan form has the eigenvalues for its diagonal entries.

11C†. Although we could give a coordinate calculation, we instead opt to give a cleaner proof. This amounts to drawing the diagram

$$\begin{tikzcd}
 & (W^\vee \otimes V) \otimes (V^\vee \otimes W) \arrow[dl, "\text{compose}"'] \arrow[d] \arrow[r, phantom, "="] & (V^\vee \otimes W) \otimes (W^\vee \otimes V) \arrow[d] \arrow[dr, "\text{compose}"] & \\
\operatorname{Hom}(W, W) \arrow[r, leftrightarrow] \arrow[dr, "\operatorname{Tr}"'] & W^\vee \otimes W \arrow[d, "\text{ev}"] & V^\vee \otimes V \arrow[r, leftrightarrow] \arrow[d, "\text{ev}"] & \operatorname{Hom}(V, V) \arrow[dl, "\operatorname{Tr}"'] \\
 & k \arrow[r, equal] & k &
\end{tikzcd}$$

It is easy to check that the center rectangle commutes, by checking it on pure tensors $\xi_W \otimes v \otimes \xi_V \otimes w$. So the outer hexagon commutes and we're done. This is really the same as the proof with bases; what it amounts to is checking the assertion is true for matrices that have a 1 somewhere and 0 elsewhere, then extending by linearity.

11D. See https://mks.mff.cuni.cz/kalva/putnam/psoln/psol886.html.

12D. Recall that (by Problem 9B[†]) we can replace "isomorphism" by "injective".

If $T(v) = 0$ for any nonzero v, then by taking a basis for which $e_1 = v$, we find $\bigwedge^n(T)$ will map $e_1 \wedge \dots$ to $0 \wedge T(e_2) \wedge \dots = 0$, hence is the zero map, so $\det T = 0$.

Conversely, if T is an isomorphism, we let S denote the inverse map. Then $1 = \det(\mathrm{id}) = \det(S \circ T) = \det S \det T$, so $\det T \neq 0$.

12E. We proceed by contradiction. Let v be a vector of length 1000 whose entries are weight of cows. Assume the existence of a matrix M such that $Mv = 0$, with entries 0 on diagonal and ±1 off-diagonal. But $\det M \pmod 2$ is equal to the number of derangements of $\{1, \dots, 1000\}$, which is odd. Thus $\det M$ is odd and in particular not zero, so M is invertible. Thus $Mv = 0 \implies v = 0$, contradiction.

12F. The answer is

$$\begin{bmatrix} t & t \\ t & t \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -3t & -t \\ t & 3t \end{bmatrix}$$

for $t \in \mathbb{R}$. These work by taking $k = 3$.

Now to see these are the only ones, consider an arithmetic matrix

$$M = \begin{bmatrix} a & a+e \\ a+2e & a+3e \end{bmatrix}.$$

with $e \neq 0$. Its characteristic polynomial is $t^2 - (2a+3e)t - 2e^2$, with discriminant $(2a+3e)^2 + 8e^2$, so it has two distinct real roots; moreover, since $-2e^2 \leq 0$ either one of the roots is zero or they are of opposite signs. Now we can diagonalize M by writing

$$M = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ps\lambda_1 - qr\lambda_2 & qs(\lambda_1 - \lambda_2) \\ pr(\lambda_2 - \lambda_1) & ps\lambda_2 - qr\lambda_1 \end{bmatrix}$$

where $ps - qr = 1$. By using the fact the diagonal entries have sum equalling the off-diagonal entries, we obtain that

$$(ps - qr)(\lambda_1 + \lambda_2) = (qs - pr)(\lambda_1 - \lambda_2) \implies qs - pr = \frac{\lambda_1 + \lambda_2}{\lambda_1 - \lambda_2}.$$

Now if $M^k \in S$ too then the same calculation gives

$$qs - pr = \frac{\lambda_1^k + \lambda_2^k}{\lambda_1^k - \lambda_2^k}.$$

Let $x = \lambda_1/\lambda_2 < 0$ (since $-2e^2 < 0$). We appropriately get

$$\frac{x+1}{x-1} = \frac{x^k+1}{x^k-1} \implies \frac{2}{x-1} = \frac{2}{x^k-1} \implies x = x^k \implies x = -1 \text{ or } x = 0$$

and k odd. If $x = 0$ we get $e = 0$ and if $x = -1$ we get $2a + 3e = 0$, which gives the curve of solutions that we claimed.

A slicker approach is by Cayley-Hamilton. Assume that $e \neq 0$, so M has two distinct real eigenvalues as above. We have $M^k = cM + d\mathrm{id}$ for some constants c and d (since M satisfies some quadratic polynomial). Since $M \in S$, $M^k \in S$ we obtain $d = 0$. Thus $M^k = cM$, so it follows the eigenvalues of M are negatives of each other. That means $\operatorname{Tr} M = 0$, and the rest is clear.

12G. Pick a basis $e_1, \dots, e_n$ of V. Let T have matrix (x_{ij}), and let $m = \dim V$. Let δ_{ij} be the Kronecker delta. Also, let $\operatorname{Fix}(\sigma)$ denote the fixed points of a permutation σ and let $\operatorname{NoFix}(\sigma)$ denote the non-fixed points.

Expanding then gives

$$\begin{aligned}
&\det(a \cdot \mathrm{id} - T) \\
&= \sum_{\sigma \in S_m} \left(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{m} \left(a \cdot \delta_{i\sigma(i)} - x_{i\sigma(i)} \right) \right) \\
&= \sum_{s=0}^{m} \sum_{1 \le i_1 < \dots < i_s \le m} \sum_{\substack{\sigma \in S_m \\ \sigma \text{ fixes } i_k}} \left(\operatorname{sign}(\sigma) \cdot \prod_{i=1}^{m} \left(a \cdot \delta_{i\sigma(i)} - x_{i\sigma(i)} \right) \right) \\
&= \sum_{s=0}^{m} \sum_{1 \le i_1 < \dots < i_s \le m} \sum_{\substack{\sigma \in S_m \\ \sigma \text{ fixes } (i_k)}} \left(\operatorname{sign}(\sigma) \cdot \prod_{i \notin (i_k)} -x_{i\sigma(i)} \prod_{i \in (i_k)}^{n} (a \cdot -x_{ii}) \right) \\
&= \sum_{\sigma \in S_m} \left(\operatorname{sign}(\sigma) \cdot \prod_{i \in \operatorname{NoFix}(\sigma)} -x_{i\sigma(i)} \prod_{i \in \operatorname{Fix}\sigma} (a - x_{ii}) \right) \\
&= \sum_{\sigma \in S_m} \left(\operatorname{sign}(\sigma) \cdot \left(\prod_{i \in \operatorname{NoFix}(\sigma)} -x_{i\sigma(i)} \right) \left(\sum_{t=0}^{|\operatorname{Fix}(\sigma)|} a^{|\operatorname{Fix}(\sigma)|-t} \cdot \sum_{i_1 < \dots < i_t \in \operatorname{Fix}(\sigma)} \prod_{k=1}^{t} -x_{i_k i_k} \right) \right) \\
&= \sum_{\sigma \in S_m} \left(\operatorname{sign}(\sigma) \left(\sum_{t=0}^{|\operatorname{Fix}(\sigma)|} a^{m-t-|\operatorname{NoFix}(\sigma)|} \sum_{\substack{X \subseteq \{1,\dots,m\} \\ \operatorname{NoFix}(\sigma) \subseteq X \\ X \text{ has exactly } t \text{ fixed}}} \prod_{i \in X} -x_{i\sigma(i)} \right) \right) \\
&= \sum_{n=0}^{m} a^{m-n} \left(\sum_{\sigma \in S_m} \operatorname{sign}(\sigma) \sum_{\substack{X \subseteq \{1,\dots,m\} \\ \operatorname{NoFix}(\sigma) \subseteq X \\ |X| = n}} \prod_{i \in X} -x_{i\sigma(i)} \right) \\
&= \sum_{n=0}^{m} a^{m-n} (-1)^n \left(\sum_{\substack{X \subseteq \{1,\dots,m\} \\ |X| = n}} \sum_{\substack{\sigma \in S_m \\ \operatorname{NoFix}(\sigma) \subseteq X}} \operatorname{sign}(\sigma) \prod_{i \in X} x_{i\sigma(i)} \right).
\end{aligned}$$

Hence it's the same to show that

$$\sum_{\substack{X \subseteq \{1,\dots,m\} \\ |X| = n}} \sum_{\substack{\sigma \in S_m \\ \operatorname{NoFix}(\sigma) \subseteq X}} \operatorname{sign}(\sigma) \prod_{i \in X} x_{i\sigma(i)} = \operatorname{Tr}_{\bigwedge^n(V)} \left(\bigwedge^n (T) \right)$$

holds for every n.

We can expand the definition of trace as using basis elements as

$$\begin{aligned}
\operatorname{Tr}\left(\bigwedge^n(T)\right) &= \sum_{1\le i_1<\dots<i_n\le m}\left(\bigwedge_{k=1}^n e_{i_k}\right)^\vee\left(\bigwedge^n(T)\left(\bigwedge_{k=1}^n e_{i_k}\right)\right)\\
&= \sum_{1\le i_1<\dots<i_n\le m}\left(\bigwedge_{k=1}^n e_{i_k}\right)^\vee\left(\bigwedge_{k=1}^n T(e_{i_k})\right)\\
&= \sum_{1\le i_1<\dots<i_n\le m}\left(\bigwedge_{k=1}^n e_{i_k}\right)^\vee\left(\bigwedge_{k=1}^n\left(\sum_{j=1}^m x_{i_kj}e_j\right)\right)\\
&= \sum_{1\le i_1<\dots<i_n\le m}\ \sum_{\pi\in S_n}\operatorname{sign}(\pi)\prod_{k=1}^n x_{i_{\pi(k)}k}\\
&= \sum_{\substack{X\subseteq\{1,\dots,m\}\\|X|=n}}\ \sum_{\pi\in S_X}\operatorname{sign}(\pi)\prod_{i\in X} x_{t\pi(t)}
\end{aligned}$$

Hence it remains to show that the permutations over X are in bijection with the permutations over S_m which fix $\{1,\dots,m\}-X$, which is clear, and moreover, the signs clearly coincide.

13C. Interpret clubs as vectors in the vector space $\mathbb{F}_2^n$. Consider a "dot product" to show that all k vectors are linearly independent: any two different club-vectors have dot product 0, while each club vector has dot product 1 with itself. So these vectors are orthonormal and hence linearly independent. Thus $k\le\dim\mathbb{F}_2^n=n$.

13D*. The inner form given by

$$\langle v_1\otimes w_1, v_2\otimes w_2\rangle_{V\otimes W}=\langle v_1,v_2\rangle_V\,\langle w_1,w_2\rangle_W$$

on pure tensors, then extending linearly. For (b) take $e_i\otimes f_j$ for $1\le i\le n$, $1\le j\le m$.

14B. Define the Boolean function $D\colon\{\pm1\}^3\to\mathbb{R}$ by

$$D(a,b,c)=ab+bc+ca=\begin{cases}3 & a,b,c\text{ all equal}\\ -1 & a,b,c\text{ not all equal.}\end{cases}.$$

Thus paradoxical outcomes arise when $D(f(x_\bullet),g(y_\bullet),h(z_\bullet))=3$. Now, we compute that for randomly selected $x_\bullet$, $y_\bullet$, $z_\bullet$ that

$$\begin{aligned}
\mathbb{E}D(f(x_\bullet),g(y_\bullet),h(z_\bullet)) &= \mathbb{E}\sum_S\sum_T\left(\widehat{f}(S)\widehat{g}(T)+\widehat{g}(S)\widehat{h}(T)+\widehat{h}(S)\widehat{f}(T)\right)(\chi_S(x_\bullet)\chi_T(y_\bullet))\\
&= \sum_S\sum_T\left(\widehat{f}(S)\widehat{g}(T)+\widehat{g}(S)\widehat{h}(T)+\widehat{h}(S)\widehat{f}(T)\right)\mathbb{E}\left(\chi_S(x_\bullet)\chi_T(y_\bullet)\right).
\end{aligned}$$

Now we observe that:

- If $S\ne T$, then $\mathbb{E}\chi_S(x_\bullet)\chi_T(y_\bullet)=0$, since if say $s\in S$, $s\notin T$ then x_s affects the parity of the product with 50% either way, and is independent of any other variables in the product.

- On the other hand, suppose $S = T$. Then
$$\chi_S(x_\bullet)\chi_T(y_\bullet) = \prod_{s\in S} x_s y_s.$$
Note that $x_s y_s$ is equal to 1 with probability $\frac13$ and -1 with probability $\frac23$ (since (x_s, y_s, z_s) is uniform from $3! = 6$ choices, which we can enumerate). From this an inductive calculation on $|S|$ gives that
$$\prod_{s\in S} x_s y_s = \begin{cases} +1 & \text{with probability } \frac12(1+(-1/3)^{|S|}) \\ -1 & \text{with probability } \frac12(1-(-1/3)^{|S|}). \end{cases}$$
Thus
$$\mathbb{E}\left(\prod_{s\in S} x_s y_s\right) = \left(-\frac13\right)^{|S|}.$$

Piecing this altogether, we now have that
$$\mathbb{E}D(f(x_\bullet), g(y_\bullet), h(z_\bullet)) = \left(\widehat{f}(S)\widehat{g}(T) + \widehat{g}(S)\widehat{h}(T) + \widehat{h}(S)\widehat{f}(T)\right)\left(-\frac13\right)^{|S|}.$$
Then, we obtain that
$$\begin{aligned}&\mathbb{E}\frac14(1 + D(f(x_\bullet), g(y_\bullet), h(z_\bullet)))\\ =&\frac14 + \frac14\sum_S \left(\widehat{f}(S)\widehat{g}(T) + \widehat{g}(S)\widehat{h}(T) + \widehat{h}(S)\widehat{f}(T)\right)\widehat{f}(S)^2\left(-\frac13\right)^{|S|}.\end{aligned}$$
Comparing this with the definition of D gives the desired result.

15B. By Theorem 9.7.6, we may select $e_1, \dots, e_n$ a basis of V and $f_1, \dots, f_m$ a basis of W such that $T(e_i) = f_i$ for $i \le k$ and $T(e_i) = 0$ for $i > k$. Then $T^\vee(f_i^\vee) = e_i^\vee$ for $i \le k$ and $T^\vee(f_i^\vee) = 0$ for $i > k$. All four quantities are above are then equal to k.

15F. First, suppose $T^* = p(T)$. Then $T^*T = p(T)\cdot T = T\cdot p(T) = TT^*$ and we're done.

Conversely, suppose T is diagonalizable in a way compatible with the inner form (OK since V is finite dimensional). Consider the orthonormal basis. Then T consists of eigenvalues on the main diagonals and zeros elsewhere, say
$$T = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$
In that case, we find that for any polynomial q we have
$$q(T) = \begin{pmatrix} q(\lambda_1) & 0 & \dots & 0 \\ 0 & q(\lambda_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & q(\lambda_n) \end{pmatrix}.$$
and
$$T^* = \begin{pmatrix} \overline{\lambda_1} & 0 & \dots & 0 \\ 0 & \overline{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \overline{\lambda_n} \end{pmatrix}.$$

So we simply require a polynomial q such that $q(\lambda_i) = \overline{\lambda_i}$ for every i. Since there are finitely many λ_i, we can construct such a polynomial using Lagrange interpolation.

16E†. https://math.stackexchange.com/a/3012179/229197

17B. Suppose $|G| = 56$ and G is simple. Consider the Sylow 7-subgroups; if there are n_7 of them we assume $n_7 > 1$ (since G is simple) and $n_7 \equiv 1 \pmod 7$, so $n_7 = 8$. That means there are $(7-1)\cdot 8 = 48$ elements of order 7 in G.

But consider the Sylow 2-subgroups. These have 8 elements each, and we conclude therefore that there is at exactly one Sylow 2-subgroup. That subgroup is normal, contradiction.

17C. One example is the group of 3×3 matrices with entries in $\mathbb{F}_3$ that are of the form $\begin{bmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{bmatrix}$.

17D. Let G be said group. If G is abelian then all subgroups are normal, and since G is simple, G can't have any subgroups at all. We can clearly find an element of order p, hence G has a subgroup of order p, which can only happen if $n = 1$, $G \cong \mathbb{Z}/p\mathbb{Z}$.

Thus it suffices to show G can't be abelian. For this, we can use the class equation, but let's avoid that and do it directly:

Assume not and let $Z(G) = \{g \in G \mid xg = gx \; \forall x \in G\}$ be the center of the group. Since $Z(G)$ is normal in G, and G is simple, we see $Z(G) = \{1_G\}$. But then let G act on itself by conjugation: $g \cdot x = gxg^{-1}$. This breaks G into a bunch of orbits $\mathcal{O}_0 = \{1_G\}$, $\mathcal{O}_1$, $\mathcal{O}_2$, $\dots$, and since 1_G is the only fixed point by definition, all other orbits have size greater than 1. The Orbit-stabilizer theorem says that each orbit now has size dividing p^n, so they must all have size zero mod p.

But then summing across all orbits (which partition G), we obtain $|G| \equiv 1 \pmod p$, which is a contradiction.

18D. Take $G = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \dots$ and $H = \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \dots$. Then there are maps $G \hookrightarrow H$ and $H \hookrightarrow G$, but the groups are not isomorphic since e.g. G has an element $g \in G$ of order 3 for which there's no $g' \in G$ with $g = 3g'$.

18E. Nope! Pick

$$\begin{aligned} A &= \mathbb{Z}[x_1, x_2, \dots] \\ B &= \mathbb{Z}[x_1, x_2, \dots, \varepsilon x_1, \varepsilon x_2, \dots] \\ C &= \mathbb{Z}[x_1, x_2, \dots, \varepsilon]. \end{aligned}$$

where $\varepsilon \neq 0$ but $\varepsilon^2 = 0$. I think the result is true if you add the assumption A is Noetherian.

19D*. The operators are those of the form $T(a) = ab$ for some fixed $b \in A$. One can check these work, since for $c \in A$ we have $T(c \cdot a) = cab = c \cdot T(a)$. To see they are the only ones, note that $T(a) = T(a \cdot 1_A) = a \cdot T(1_A)$ for any $a \in A$.

20C. Pick any $v \in V$, then the subspace spanned by elements $g \cdot v$ for $v \in V$ is G-invariant; this is a finite-dimensional subspace, so it must equal all of V.

21B. $\mathbb{C}_{\text{sign}} \oplus \mathbb{C}^2 \oplus \text{refl}_0 \oplus (\text{refl}_0 \otimes \mathbb{C}_{\text{sign}})$.

21C. First, observe that $|\chi_W(g)| = 1$ for all $g \in G$.

$$\begin{aligned}\langle \chi_{V\otimes W}, \chi_{V\otimes W}\rangle &= \langle \chi_V\chi_W, \chi_V\chi_W\rangle \\ &= \frac{1}{|G|}\sum_{g\in G} |\chi_V(g)|^2 \, |\chi_W(g)|^2 \\ &= \frac{1}{|G|}\sum_{g\in G} |\chi_V(g)|^2 \\ &= \langle \chi_V, \chi_V\rangle = 1.\end{aligned}$$

21D. The table is given by

Q_8	1	-1	$\pm i$	$\pm j$	$\pm k$
$\mathbb{C}_{\text{triv}}$	1	1	1	1	1
$\mathbb{C}_i$	1	1	1	-1	-1
$\mathbb{C}_j$	1	1	-1	1	-1
$\mathbb{C}_k$	1	1	-1	-1	1
$\mathbb{C}^2$	2	-2	0	0	0

The one-dimensional representations (first four rows) follows by considering the homomorphism $Q_8 \to \mathbb{C}^\times$. The last row is two-dimensional and can be recovered by using the orthogonality formula.

23A. By a straightforward computation, we have $|\Psi_-\rangle = -\frac{1}{\sqrt{2}}\left(|{\to}\rangle_A \otimes |{\leftarrow}\rangle_B - |{\leftarrow}\rangle_A |{\to}\rangle_B\right)$. Now, $|{\to}\rangle_A \otimes |{\to}\rangle_B$, $|{\to}\rangle_A \otimes |{\leftarrow}\rangle_B$ span one eigenspace of $\sigma_x^A \otimes \operatorname{id}_B$, and $|{\leftarrow}\rangle_A \otimes |{\to}\rangle_B$, $|{\leftarrow}\rangle_A \otimes |{\leftarrow}\rangle_B$ span the other. So this is the same as before: $+1$ gives $|{\leftarrow}\rangle_B$ and -1 gives $|{\leftarrow}\rangle_A$.

24A. To show the Fredkin gate is universal it suffices to reversibly create a CCNOT gate with it. We write the system

$$\begin{aligned}(z, \neg z, -) &= \operatorname{Fred}(z, 1, 0) \\ (x, a, -) &= \operatorname{Fred}(x, 1, 0) \\ (y, b, -) &= \operatorname{Fred}(y, a, 0) \\ (-, c, -) &= \operatorname{Fred}(b, 0, 1) \\ (-, d, -) &= \operatorname{Fred}(c, z, \neg z).\end{aligned}$$

Direct computation shows that $d = z + xy \pmod 2$.

24C. Put $|{\leftarrow}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Then we have that U_f sends

$$|x_1\rangle \dots |x_m\rangle |0\rangle - |x_1\rangle \dots |x_m\rangle |1\rangle \xmapsto{U_f} \pm |x_1\rangle \dots |x_m\rangle |0\rangle \mp |x_1\rangle \dots |x_m\rangle |1\rangle$$

the sign being $+$, $-$ exactly when $f(x_1, \dots, x_m) = 1$.

Now, upon inputting $|0\rangle \dots |0\rangle |1\rangle$, we find that $H^{\otimes m+1}$ maps it to

$$2^{-n/2} \sum_{x_1,\dots,x_n} |x_1\rangle \dots |x_n\rangle |{\leftarrow}\rangle .$$

Then the image under U_f is

$$2^{-n/2} \sum_{x_1,\dots,x_n} (-1)^{f(x_1,\dots,x_n)} |x_1\rangle \dots |x_n\rangle |{\leftarrow}\rangle .$$

We now discard the last qubit, leaving us with

$$2^{-n/2} \sum_{x_1,\dots,x_n} (-1)^{f(x_1,\dots,x_n)} |x_1\rangle \dots |x_n\rangle .$$

Applying $H^{\otimes m}$ to this, we get

$$2^{-n/2} \sum_{x_1,\dots,x_n} (-1)^{f(x_1,\dots,x_n)} \cdot \left(2^{-n/2} \sum_{y_1,\dots,y_n} (-1)^{x_1y_1+\dots+x_ny_n} |y_1\rangle |y_2\rangle \dots |y_n\rangle \right)$$

since $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ while $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, so minus signs arise exactly if $x_i = 1$ and $y_i = 1$ simultaneously, hence the term $(-1)^{x_1y_1+\dots+x_ny_n}$. Swapping the order of summation, we get

$$2^{-n} \sum_{y_1,\dots,y_n} C(y_1,\dots,y_n) |y_1\rangle |y_2\rangle \dots |y_n\rangle$$

where $C_{y_1,\dots,y_n} = \sum_{x_1,\dots,x_n} (-1)^{f(x_1,\dots,x_n)+x_1y_1+\dots+x_ny_n}$. Now, we finally consider two cases.

- If f is the constant function, then we find that

  $$C(y_1,\dots,y_n) = \begin{cases} \pm 1 & y_1 = \dots = y_n = 0 \\ 0 & \text{otherwise.} \end{cases}$$

  To see this, note that the result is clear for $y_1 = \dots = y_n = 0$; otherwise, if WLOG $y_1 = 1$, then the terms for $x_1 = 0$ exactly cancel the terms for $x_1 = 1$, pair by pair. Thus in this state, the measurements all result in $|0\rangle \dots |0\rangle$.

- On the other hand if f is balanced, we derive that

  $$C(0,\dots,0) = 0.$$

  Thus *no* measurements result in $|0\rangle \dots |0\rangle$.

In this way, we can tell whether f is balanced or not.

26E. This is an application of Cauchy convergence, since one can show that

$$\left| \sum_{n=M}^{N} (-1)^n a_n \right| \le a_{\min\{M,N\}}.$$

Indeed, if M and N are even (for simplicity; other cases identical) then

$$\begin{aligned} a_M - a_{M+1} + a_{M+2} - \dots &= a_M - (a_{M+1} - a_{M+2}) - (a_{M+3} - a_{M+4}) \\ &\quad - \dots - (a_{N-1} - a_N) \\ &\le a_M \\ a_M - a_{M+1} + a_{M+2} - \dots &= a_M - a_{M+1} + (a_{M+2} - a_{M+3}) + (a_{M+4} - a_{M+5}) \\ &\quad + \dots + (a_{N-2} - a_{N+1}) + a_N \\ &\ge -a_{M+1}. \end{aligned}$$

In this way we see that the sequence of partial sums is Cauchy, hence converges to some limit.

26F. To capture the hypothesis of monotonic and bounded, write $a_n = x_1 + \dots + x_n$ for some x_i. Then x_2, ... are all the same sign and so $\sum |x_i| = A < \infty$ for some constant A.

We now prove that the partial sums of $\sum a_n b_n$ are a Cauchy sequence. Consider any $\varepsilon > 0$. Let K be such that the tails of b_n starting after K have absolute value less than $\frac{\varepsilon}{A}$. Then for any $N > M \ge K$ we have

$$\begin{aligned} \left| \sum_{k=M}^{N} a_k b_k \right| &= \left| \sum_{k=M}^{N} \sum_{j=1}^{k} b_k x_j \right| \\ &= \left| \sum_{j=1}^{N} \sum_{k=\max\{j,M\}}^{N} b_k x_j \right| \\ &= \left| \sum_{j=1}^{N} x_j \cdot \sum_{k=\max\{j,M\}}^{N} b_k \right| \\ &\le \sum_{j=1}^{N} |x_j| \left| \sum_{k=\max\{j,M\}}^{N} b_k \right| \\ &< \sum_{j=1}^{N} |x_j| \cdot \frac{\varepsilon}{A} \\ &< \varepsilon \end{aligned}$$

as desired.

26G. The answer is $e - 1$.

We begin by noting $x_{n+1} = \log(e^{x_n} - x_n) \ge \log 1 = 0$, owing to $e^t \ge 1 + t$. So $x_n \ge 0$ for all n.

Next notice that

$$x_{n+1} = \log\left(e^{x_n} - x_n\right) < \log e^{x_n} = x_n.$$

So x_1, x_2, ... is strictly decreasing in addition to nonnegative. Thus it must converge to some limit L.

Third, observe that

$$x_n = e^{x_n} - e^{x_{n+1}} \implies x_0 + x_1 + \dots + x_n = e^{x_0} - e^{x_n} = e - e^{x_n} < e.$$

Since the partial sums are bounded by e, and $x_i \ge 0$, we conclude $L = 0$.

Finally, the limit of the partial sums is then

$$\lim_{n\to\infty} e - e^{x_n} = e - e^0 = e - 1.$$

28G. Write $f(x) = e^{x \log x}$ and then apply the chain rule and product rule:

$$\begin{aligned} f'(x) &= e^{x \log x} \cdot (x \log x)' \\ &= e^{x \log x} \cdot (1 + \log x) \\ &= x^x \left(1 + \log x\right). \end{aligned}$$

29E. See `https://mathoverflow.net/q/81613` and in particular `https://web.archive.org/web/20161009194815/http://mathforum.org/kb/message.jspa?messageID=387148`.

31B*. Proceed by contradiction, meaning there exists a sequence $z_1, z_2, \dots \to z$ where $0 = f(z_1) = f(z_2) = \dots$ all distinct. WLOG set $z = 0$. Look at the Taylor series of f around $z = 0$. Since it isn't uniformly zero by assumption, write it as $a_N z^N + a_{N+1} z^{N+1} + \cdots$, $a_N \neq 0$. But by continuity of $h(z) = a_N + a_{N+1} z + \cdots$ there is some open neighborhood of zero where $h(z) \neq 0$.

31C*. Let S be the interior of the points satisfying $f = g$. By definition S is open. By the previous part, S is closed: if $z_i \to z$ and $z_i \in S$, then $f = g$ in some open neighborhood of z, hence $z \in S$. Since S is clopen and nonempty, $S = U$.

31E. Suppose we want to show that there's a point in the image within ε of a given a point $w \in \mathbb{C}$. Look at $\frac{1}{f(z)-w}$ and use Liouville's theorem.

32C. See https://math.stackexchange.com/q/242514/229197, which does it with 2019 replaced by 3.

39A. It is the counting measure.

41A. For each positive integer m, consider what happens when $\varepsilon = 1/m$. Then, by hypothesis, there is a threshold N_m such that the *anomaly set*

$$A_m := \left\{ \omega : |X(\omega) - X_n(\omega)| \geq \frac{1}{m} \text{ for some } n > N_m \right\}$$

has measure $\mu(A_m) = 0$. Hence, the countable union $A = \bigcup_{m \geq 1} A_m$ has measure zero too.

So the complement of A has measure 1. For any world $\omega \notin A$, we then have

$$\lim_n |X(\omega) - X_n(\omega)| = 1$$

because when $n > N_m$ that absolute value is always at most $1/m$ (as $\omega \notin A_m$).

41B. https://math.stackexchange.com/a/2201906/229197

55C. If $\alpha \equiv 0 \pmod{\mathfrak{p}}$ it's clear, so assume this isn't the case. Then $\mathcal{O}_K/\mathfrak{p}$ is a finite field with $\mathrm{N}(\mathfrak{p})$ elements. Looking at $(\mathcal{O}_K/\mathfrak{p})^*$, it's a multiplicative group with $\mathrm{N}(\mathfrak{p}) - 1$ elements, so $\alpha^{\mathrm{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$, as desired.

55D†. Suppose it's generated by some elements in K; we can write them as $\frac{\beta_i}{\alpha_i}$ for $\alpha_i, \beta_i \in \mathcal{A}$. Hence

$$J = \left\{ \sum_i \gamma_i \cdot \frac{\beta_i}{\alpha_i} \mid \alpha_i, \beta_i, \gamma_i \in \mathcal{O}_K \right\}.$$

Now "clear denominators". Set $\alpha = \alpha_1 \dots \alpha_n$, and show that αJ is an integral ideal.

55E. For part (a), note that the $\mathfrak{p}_i$ are prime just because

$$\mathcal{O}_K/\mathfrak{p}_i \cong (\mathbb{Z}[x]/f)/(p, f_i) \cong \mathbb{F}_p[x]/(f_i)$$

is a field, since the f_i are irreducible.

We check (b). Computing the product modulo p yields[2]

$$\prod_{i=1}^{g} (f_i(\theta))^{e_i} \equiv (f(\theta)) \equiv 0 \pmod{p}$$

[2] For example, suppose we want to know that $(3, 1+\sqrt{7})(3, 1-\sqrt{7})$ is contained in (3). We could do the full computation and get $(9, 3+3\sqrt{7}, 3-3\sqrt{7}, 6)$. But if all we care about is that every element is divisible by 3, we could have just taken "mod 3" at the beginning and looked at just $(1+\sqrt{7})(1-\sqrt{7}) = (6)$; all the other products we get will obviously have factors of 3.

so we've shown that $I \subseteq (p)$.

Finally, we prove (c) with a size argument. The idea is that I and (p) really should have the same size; to nail this down we'll use the ideal norm. Since (p) divides I, we can write $(p) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i'}$ where $e_i' \le e_i$ for each i. Remark $\mathcal{O}_K/(p) \cong \mathbb{Z}/p\mathbb{Z}[x]/(f)$ has size $p^{\deg f}$. Similarly, $\mathcal{O}_K/(\mathfrak{p}_i)$ has degree $p^{\deg f_i}$ for each i. Compute $\mathrm{N}((p))$ using the e_i' now and compare the results.

56F. Let $K = \mathbb{Q}(\sqrt{-5})$. Check that Cl_K has order two using the Minkowski bound; moreover $\Delta_K = 20$. Now note that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and x^2+5 factors mod p as $(x+k)(x-k)$; hence in $\mathcal{O}_K$ we have $(p) = (p, \sqrt{-5}+k)(p, \sqrt{-5}-k) = \mathfrak{p}_1\mathfrak{p}_2$, say. For $p > 5$ the prime p does not ramify and we have $\mathfrak{p}_1 \ne \mathfrak{p}_2$, since $\Delta_K = 20$.

Then $(p^2) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$. Because the class group has order two, both $\mathfrak{p}_1^2$ and $\mathfrak{p}_2^2$ are principal, and because $\mathfrak{p}_1 \ne \mathfrak{p}_2$ they are distinct. Thus p^2 is a nontrivial product of two elements of $\mathcal{O}_K$; from this we can extract the desired factorization.

59A*. It's just $\mathbb{Z}/p-1\mathbb{Z}$, since ζ_p needs to get sent to one (any) of the $p-1$ primitive roots of unity.

59D. A similar (but not identical) problem is solved here: https://aops.com/community/c6h149153p842956.

59F. https://www.math.cornell.edu/~kbrown/6310/primitive.pdf

60A†. Recall that the Fibonacci sequence is given by

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the two roots of $P(X) := X^2 - X - 1$.

Let $p = 127$ and work modulo p. As

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$$

we see 5 is not a quadratic residue mod 127. Thus the polynomial $P(X)$, viewed as a polynomial in $\mathbb{F}_p[X]$, is irreducible (intuitively, α and β are not elements of $\mathbb{F}_p$). Accordingly we will work in the finite field $\mathbb{F}_{p^2}$, which is the $\mathbb{F}_p$-splitting field of $P(X)$. In other words we interpret α and β as elements of $\mathbb{F}_{p^2}$ which do not lie in $\mathbb{F}_p$.

Let $\sigma\colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ by $t \mapsto t^p$ be the nontrivial element of $\mathrm{Gal}\left(\mathbb{F}_{p^2}/\mathbb{F}_p\right)$; in other words, σ is the non-identity automorphism of $\mathbb{F}_{p^2}$. Since the fixed points of σ are the elements of $\mathbb{F}_p$, this means σ does not fix either root of P; thus we must have

$$\begin{aligned} \alpha^p &= \sigma(\alpha) = \beta \\ \beta^p &= \sigma(\beta) = \alpha. \end{aligned}$$

Now, compute

$$\begin{aligned} F_p &= \frac{\alpha^p - \beta^p}{\alpha - \beta} = \frac{\beta - \alpha}{\alpha - \beta} = -1. \\ F_{p+1} &= \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = \frac{\alpha\beta - \beta\alpha}{\alpha - \beta} = 0. \\ F_{2p+1} &= \frac{\alpha^{2p+1} - \beta^{2p+1}}{\alpha - \beta} = \frac{\beta^2\alpha - \alpha^2\beta}{\alpha - \beta} = -\alpha\beta = 1. \\ F_{2p+2} &= \frac{\alpha^{2p+2} - \beta^{2p+2}}{\alpha - \beta} = \frac{\beta^2\alpha^2 - \alpha^2\beta^2}{\alpha - \beta} = 0. \end{aligned}$$

Consequently, the period must divide $2p+2$ but not $p+1$.

We now use for the first time the exact numerical value $p = 127$ to see the period divides $2p + 2 = 256 = 2^8$, but not $p + 1 = 128 = 2^7$. (Previously we only used the fact that $(5/p) = -1$.) Thus the period must be exactly 256.

62A. It is still true that

$$\left(\frac{2}{q}\right) = 1 \iff \sigma_2 \in H \iff 2 \text{ splits in } \mathbb{Z}\left[\tfrac{1}{2}(1+\sqrt{q^*})\right].$$

Now, 2 splits in the ring if and only if $t^2 - t - \frac{1}{4}(1 - q^*)$ factors mod 2. This happens if and only if $q^* \equiv 1 \pmod 8$. One can check this is exactly if $q \equiv \pm 1 \pmod 8$, which gives the conclusion.

62C†. Let $K = \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. One can show that $\operatorname{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ exactly as before. In particular, $\operatorname{Gal}(K/\mathbb{Q})$ is abelian and therefore its conjugacy classes are singleton sets; there are $\phi(m)$ of them.

As long as p is sufficiently large, it is unramified and $\sigma_p = \operatorname{Frob}_{\mathfrak{p}}$ for any $\mathfrak{p}$ above p (as mth roots of unity will be distinct modulo p; differentiate $x^m - 1$ mod p again).

62E. This solution is by David Corwin. By primitive roots, it's the same as the action of ×3 on $\mathbb{Z}/(p-1)\mathbb{Z}$. Let ζ be a $(p-1)$st root of unity.

Consider

$$d = \prod_{0 \le i < j < p-1} (\zeta^i - \zeta^j).$$

This is the square root of the discriminant of the polynomial $X^{p-1} - 1$; in other words $d^2 \in \mathbb{Z}$. In fact, by elementary methods one can compute

$$(-1)^{\binom{p-1}{2}} d^2 = -(p-1)^{p-1}$$

Now take the extension $K = \mathbb{Q}(d)$, noting that

- If $p \equiv 3 \pmod 4$, then $d = (p-1)^{\frac{1}{2}(p-1)}$, so $K = \mathbb{Q}$.
- If $p \equiv 1 \pmod 4$, then $d = i(p-1)^{\frac{1}{2}(p-1)}$, so $K = \mathbb{Q}(i)$.

Either way, in $\mathcal{O}_K$, let $\mathfrak{p}$ be a prime ideal above $(3) \subseteq \mathcal{O}_K$. Let $\sigma = \operatorname{Frob}_{\mathfrak{p}}$ then be the unique element such that $\sigma(x) = x^3 \pmod{\mathfrak{p}}$ for all x. Then, we observe that

$$\sigma(d) \equiv \prod_{0 \le i < j < p-1} (\zeta^{3i} - \zeta^{3j}) \equiv \begin{cases} +d & \text{if } \pi \text{ is even} \\ -d & \text{if } \pi \text{ is odd} \end{cases} \pmod{\mathfrak{p}}.$$

Now if $K = \mathbb{Q}$, then σ is the identity, thus σ even. Conversely, if $K = \mathbb{Q}(i)$, then 3 does not split, so $\sigma(d) = -d$ (actually σ is complex conjugation) thus π is odd.

Note the condition that $p \equiv 2 \pmod 3$ is used only to guarantee that π is actually a permutation (and thus $d \neq 0$); it does not play any substantial role in the solution.

63A†. Suppose $\mathfrak{f}(L/\mathbb{Q}) \mid m\infty$ for some m. Then by the example from earlier we have the chain

$$P_{\mathbb{Q}}(m\infty) = H(\mathbb{Q}(\zeta)/\mathbb{Q}, m\infty) \subseteq H(L/\mathbb{Q}, m) \subseteq I_{\mathbb{Q}}(m\infty).$$

So by inclusion reversal we're done.

63B†. Apply the Takagi existence theorem with $\mathfrak{m} = 1$ to obtain an unramified extension E/K such that $H(E/K, 1) = P_K(1)$. We claim this works:

- To see it is maximal by inclusion, note that any other extension M/K with this property has conductor 1 (no primes divide the conductor), and then we have $P_K(1) = H(E/K, 1) \subseteq H(M/K, 1) \subseteq I_K(1)$, so inclusion reversal gives $M \subseteq E$.
- We have $\operatorname{Gal}(L/K) \cong I_K(1)/P_K(1) = C_K(1)$ the class group.
- The isomorphism in the previous part is given by the Artin symbol. So $\mathfrak{p}$ splits completely if and only if $\left(\frac{L/K}{\mathfrak{p}}\right) = \operatorname{id}$ if and only if $\mathfrak{p}$ is principal (trivial in $C_K(1)$).

This completes the proof.

68A. The main observation is that in $\mathcal{A} \times \mathbf{2}$, you have the arrows in $\mathcal{A}$ (of the form $(f, \operatorname{id}_{\mathbf{2}})$), and then the arrows crossing the two copies of $\mathcal{A}$ (of the form $(\operatorname{id}_A, 0 \le 1)$). But there are some more arrows $(f, 0 \le 1)$: nonetheless, they can be thought of as compositions

$$(f, 0 \le 1) = (f, \operatorname{id}_{\mathbf{2}}) \circ (\operatorname{id}_A, 0 \le 1) = (\operatorname{id}_A, 0 \le 1) \circ (f, \operatorname{id}_{\mathbf{2}}).$$

Now to specify a functor $\alpha \colon \mathcal{A} \times \mathbf{2} \to \mathcal{B}$, we only have to specify where each of these two more basic things goes. The conditions on α already tells us that $(f, \operatorname{id}_{\mathbf{2}})$ should be mapped to $F(f)$ or $G(f)$ (depending on whether the arrow above is in $\mathcal{A} \times \{0\}$ or $\mathcal{A} \times \{1\}$), and specifying the arrow $(\operatorname{id}_A, 0 \le 1)$ amounts to specifying the Ath component. Where does naturality come in?

The above discussion transfers to products of categories in general: you really only have to think about (f, id) and (id, g) arrows to get the general arrow $(f, g) = (f, \operatorname{id}) \circ (\operatorname{id}, g) = (\operatorname{id}, g) \circ (f, \operatorname{id})$.

70A. Let $c \in C$ with $\gamma(c) = 0$. We show $c = 0$. This proceeds in a diagram chase:

- Note that $0 = r'(\gamma(c)) = \delta(r(c))$, and since δ is injective, it follows that $r(c) = 0$.
- Since the top row is exact, it follows $c = q(b)$ for some $b \in B$.
- Then $q'(\beta(b)) = 0$, so if we let $b' = \beta(b)$, then $b' \in \ker(q')$. As the bottom row is exact, there exists a' with $p'(a') = b'$.
- Since α is injective, there is $a \in A$ with $\alpha(a) = a'$.
- Since β is injective, it follows that $p(a) = b$.
- Since the top row is exact, and b is in the image of p, it follows that $0 = q(b) = c$ as needed.

71A. Applying the functor H_{n-1} we get that the composition $\mathbb{Z} \to 0 \to \mathbb{Z}$ is the identity which is clearly not possible.

72B. The answer is $\widetilde{H}_{n-1}(X) \cong \mathbb{Z}^{\oplus p}$, with all other groups vanishing. For $p = 1$, $\mathbb{R}^n - \{*\} \cong S^{n-1}$ so we're done. For all other p, draw a hyperplane dividing the p points into two halves with a points on one side and b points on the other (so $a + b = p$). Set U and V and use induction.

Alternatively, let U be the desired space and let V be the union of p disjoint balls, one around every point. Then $U \cup V = \mathbb{R}^n$ has all reduced homology groups trivial. From the Mayer-Vietoris sequence we can read $\widetilde{H}_k(U \cap V) \cong \widetilde{H}_k(U) \cap \widetilde{H}_k(V)$. Then $U \cap V$ is p punctured balls, which are each the same as S^{n-1}. One can read the conclusion from here.

72C*. It is $\mathbb{Z}$ for $k = n$ and 0 otherwise.

72F*. Use the short exact sequence

$$0 \to C_\bullet(B, A) \to C_\bullet(X, A) \to C_\bullet(X, B) \to 0$$

of chain complexes.

73B. We have an exact sequence

$$\underbrace{\widetilde{H}_1(\mathbb{R})}_{=0} \to \widetilde{H}_1(\mathbb{R}, \mathbb{Q}) \to \widetilde{H}_0(\mathbb{Q}) \to \underbrace{\widetilde{H}_0(\mathbb{R})}_{=0}.$$

Now, since $\mathbb{Q}$ is path-disconnected (i.e. no two of its points are path-connected) it follows that $\widetilde{H}_0(\mathbb{Q})$ consists of countably infinitely many copies of $\mathbb{Z}$.

73E. This is shown in detail in Section 2.B of Hatcher.

74D. For concreteness, let's just look at the homology at $H_2(X^2, X^1)$ and show it's isomorphic to $H_2(X)$. According to the diagram

$$\begin{aligned} H_2(X) &\cong H_2(X^3) \\ &\cong H_2(X^2)/\ker\left[H_2(X^2) \twoheadrightarrow H_2(X^3)\right] \\ &\cong H_2(X^2)/\operatorname{im}\partial_3 \\ &\cong \operatorname{im}\left[H_2(X^2) \hookrightarrow H_2(X^2, X^1)\right]/\operatorname{im}\partial_3 \\ &\cong \ker(\partial_2)/\operatorname{im}\partial_3 \\ &\cong \ker d_2/\operatorname{im} d_3. \end{aligned}$$

76D. See [Ma13a, Example 3.3.14, pages 68-69].

77B. If $V = \mathcal{V}(I)$ with $I = (f_1, \dots, f_m)$ (as usual there are finitely many polynomials since $\mathbb{R}[x_1, \dots, x_n]$ is Noetherian) then we can take $f = f_1^2 + \dots + f_m^2$.

77C. Let I be an ideal, and let $\mathfrak{m}$ be a maximal ideal contained in it. (If you are worried about the existence of $\mathfrak{m}$, it follows from Krull's Theorem, Problem 5E*). Then $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ by Weak Nullstellensatz. Consequently, $(a_1, \dots, a_n)$ is the unique point of $\mathcal{V}(\mathfrak{m})$, and hence this point is also in $\mathcal{V}(I)$.

77D. The point is to check that if f vanishes on all of $\mathcal{V}(I)$, then $f \in \sqrt{I}$.

Take a set of generators $f_1, \dots, f_m$, in the original ring $\mathbb{C}[x_1, \dots, x_n]$; we may assume it's finite by the Hilbert basis theorem.

We're going to do a trick now: consider $S = \mathbb{C}[x_1, \dots, x_n, x_{n+1}]$ instead. Consider the ideal $I' \subseteq S$ in the bigger ring generated by $\{f_1, \dots, f_m\}$ and the polynomial $x_{n+1}f - 1$. The point of the last guy is that its zero locus does not touch our copy $x_{n+1} = 0$ of $\mathbb{A}^n$ nor any point in the "projection" of f through $\mathbb{A}^{n+1}$ (one can think of this as $\mathcal{V}(I)$ in the smaller ring direct multiplied with $\mathbb{C}$). Thus $\mathcal{V}(I') = \varnothing$, and by the weak Nullstellensatz we in fact have $I' = \mathbb{C}[x_1, \dots, x_{n+1}]$. So

$$1 = g_1 f_1 + \dots + g_m f_m + g_{m+1}\left(x_{n+1}f - 1\right).$$

Now the hack: **replace every instance of x_{n+1} by $\frac{1}{f}$**, and then clear all denominators. Thus for some large enough integer N we can get

$$f^N = f^N(g_1 f_1 + \dots + g_m f_m)$$

which eliminates any fractional powers of f in the right-hand side. It follows that $f^N \in I$.

80A. From the exactness, $h_I(d) = h_I(d-k) + h_{I+(f)}(d)$, and it follows that

$$\chi_{I+(f)}(d) = \chi_I(d) - \chi_I(d-k).$$

Let $m = \dim \mathcal{V}_{\text{pr}}(I) \geq 1$. Now $\dim \mathcal{V}_{\text{pr}}(I + (f)) = m - 1$, so and $c_{\text{new}} = \deg I + (f)$ then we have

$$\frac{\deg(I+(f))d^{m-1} + \dots}{(m-1)!} = \frac{1}{m!}\left(\deg I(d^m - (d-k)^m) + \text{lower order terms}\right)$$

from which we read off

$$\deg(I + (f)) = \frac{(m-1)!}{m!} \cdot k\binom{m}{1}\deg I = k \deg I$$

as needed.

80B. In complex numbers with ABC the unit circle, it is equivalent to solving the two cubic equations

$$\begin{aligned}(p-a)(p-b)(p-c) &= (abc)^2(q - 1/a)(q-1/b)(q-1/c)\\ 0 &= \prod_{\text{cyc}}(p + c - b - bcq) + \prod_{\text{cyc}}(p + b - c - bcq)\end{aligned}$$

in p and $q = \overline{p}$. Viewing this as two cubic curves in $(p, q) \in \mathbb{C}^2$, by Bézout's theorem it follows there are at most nine solutions (unless both curves are not irreducible, but one can check the first one cannot be factored). Moreover it is easy to name nine solutions (for ABC scalene): the three vertices, the three excenters, and I, O, H. Hence the answer is just those three triangle centers I, O and H.

81C. If they were isomorphic, we would have $\mathcal{O}_V(V) \cong \mathcal{O}_W(W)$. For irreducible projective varieties, $\mathcal{O}_W(W) \cong \mathbb{C}$, while for affine varieties $\mathcal{O}_V(V) \cong \mathbb{C}[V]$. Thus we conclude V must be a single point.

81D. Assume for contradiction there is an affine variety V and an isomorphism

$$f\colon X \to V.$$

Then taking the pullback we get a ring isomorphism

$$f^\sharp\colon \mathcal{O}_V(V) \to \mathcal{O}_X(X) = \mathbb{C}[x,y].$$

Now let $\mathcal{O}_V(V) = \mathbb{C}[a,b]$ where $f^\sharp(a) = x$, $f^\sharp(b) = y$. In particular, we actually have to have $V \cong \mathbb{A}^2$.

Now in the *affine* variety V we can take $\mathcal{V}(a)$ and $\mathcal{V}(b)$; these have nonempty intersection since (a,b) is a maximal ideal in $\mathcal{O}_V(V)$. Call this point q, and let p be a point with $f(p) = q$.

Then

$$0 = a(q) = (f^\sharp a)(p) = x(p)$$

and so $p \in \mathcal{V}(x) \subseteq X$. Similarly, $p \in \mathcal{V}(y) \subseteq X$, but this is a contradiction since $\mathcal{V}(x,y) = \varnothing$.

82A. Because the stalks are preserved by sheafification, there is essentially nothing to prove: both sides correspond to sequences of compatible $\mathscr{F}$-germs over U.

83A. One should get $A[1/60] = \mathbb{Z}/7\mathbb{Z}$.

83B. If and only if S has no zero divisors.

83D. Take $A = \mathbb{C}[x,y]/(xy)$.

85B. Let $V = D(x) \cup D(y) \subset U$ denote the punctured plane, so its complement $D(z)$ looks like a punctured line. Then $V \cap D(z) = \varnothing$ and the following diagram of restriction maps commutes

$$\begin{tikzcd}
 & \mathcal{O}_X(X) = A \arrow[d] \arrow[ddl] \arrow[ddr] & \\
 & \mathcal{O}_X(U) \arrow[dl] \arrow[dr] & \\
\mathcal{O}_X(D(z)) \arrow[dr] & & \mathcal{O}_X(V) \arrow[dl] \\
 & \mathcal{O}_X(\varnothing) = 0 &
\end{tikzcd}$$

By sheaf axioms we should actually have

$$\mathcal{O}_X(U) = \mathcal{O}_X(D(z)) \times \mathcal{O}_X(V).$$

We have $\mathcal{O}_X(D(z)) = A_z = k[x,y,z,z^{-1}]/(xz,yz) \cong k[z,z^{-1}]$. On the other hand $\mathcal{O}_X(V) = k[x,y]$ as shown in §4.4.1 of Vakil. So

$$\mathcal{O}_X(U) = k[x,y] \times k[z,z^{-1}].$$

87A. Since $\mathbb{Z}$ is the initial object of CRing, it follows $\operatorname{Spec}\mathbb{Z}$ is the final object of AffSch. $\mathfrak{p}$ gets sent to the characteristic of the field $\mathcal{O}_{X,\mathfrak{p}}/\mathfrak{m}_{X,\mathfrak{p}}$.

88A. Let $\varepsilon = \pi - 3.141592653 < 10^{-9}$. Then

$$\frac{22}{7} = f(\pi) = f(3.141592653) + f(\varepsilon) = 3.141592653 + f(\varepsilon).$$

Therefore,

$$f(\varepsilon) = \frac{22}{7} - 3.141592653 = \frac{22 - 21.991148571}{7} > \frac{0.008}{7} > 10^{-3}.$$

So

$$f(10^8\varepsilon) = 10^8 f(\varepsilon) > 10^5 > 9000$$

and $10^8\varepsilon < 1$, as needed.

88B. Every statement is true.

The first statement follows by simply extending f via

$$x \mapsto \begin{cases} f(x) & x > 0 \\ 0 & x = 0 \\ -f(-x) & x < 0. \end{cases}$$

The second statement is true for any additive function $\mathbb{R} \to \mathbb{R}$. Indeed, $f(0) = f(0) + f(0) \implies f(0) = 0$, and odd follows.

The third and fourth statement follow from https://en.wikipedia.org/wiki/Cauchy%27s_functional_equation#Properties_of_nonlinear_solutions_over_the_real_numbers.

The fifth statement is kind of stupid. If f was surjective, there should exist $a > 0$ such that $f(a) = 0$. But then $f(2a) = f(a) + f(a) = 0$, so f is not injective.

For the rest, fix a Hamel basis

$$E = \{e_\alpha \mid \alpha \in S := \{0, 1, 2, \dots\} \dots\}.$$

Here S is an uncountable set of ordinals. WLOG, $e_0 = 1$ and $e_\alpha > 0$ for all $\alpha \in S$. Then f is uniquely determined by the value of $f(e_\alpha)$ for each $\alpha \in S$.

- For the sixth statement, let $f(e_0) = e_1$, $f(e_1) = e_0$, and $f(e_\alpha) = e_\alpha$ for all other $\alpha \geq 2$.
- The seventh statement is the most complicated. Since S is infinite, it's possible to construct a 2-to-1 map $\psi \colon S \to S$, meaning every element of the codomain is the image of exactly two elements in the domain. Then if $\psi(\alpha) = \psi(\beta) = \gamma$ for $\alpha \neq \beta$, set $f(e_\alpha) = e_\gamma$, $f(e_\beta) = -e_\gamma$.
- For the eighth statement, let $f(e_\alpha) = 1$ for every $\alpha \in S$.
- For the ninth statement, let $f(e_\alpha) = \sqrt{2}$ for every $\alpha \in S$.

89E. Define an equivalence relation equating two hat configurations if they differ in only finitely many places. Now for each equivalence class, everyone pre-agrees on a particular representative. Finally, note that a person can determine which equiv class the group is in even without their own hat color. Hence they unanimously select the same representative, QED.

92C†. For a sentence ϕ let

$$f_\phi \colon \kappa \to \kappa$$

send α to the least $\beta < \kappa$ such that for all $\vec{b} \in V_\alpha$, if there exists $a \in V_\kappa$ such that $V_\kappa \vDash \phi[a, \vec{b}]$ then $\exists a \in V_\beta$ such that $V_\kappa \vDash \phi[a, \vec{b}]$.

We claim this is well-defined. There are only $|V_\alpha|^n$ many possible choices of $\vec{b}$, and in particular there are fewer than κ of these (since we know that $|V_\alpha| < \kappa$; compare Problem 91C*). Otherwise, we can construct a cofinal map from $|V_\alpha^n|$ into κ by mapping each vector $\vec{b}$ into a β for which the proposition fails. And that's impossible since κ is regular!

In other words, what we've done is fix ϕ and then use Tarski-Vaught on all the $\vec{b} \in V_\alpha^n$. Now let $g \colon \kappa \to \kappa$ be defined by

$$\alpha \mapsto \sup f_\phi(\alpha).$$

Since κ is regular and there are only countably many formulas, $g(\alpha)$ is well-defined.

Check that if α has the property that g maps α into itself (in other words, α is closed under g), then by the Tarski-Vaught test, we have $V_\alpha \prec V_\kappa$.

So it suffices to show there are arbitrarily large $\alpha < \kappa$ which are closed under g. Fix α_0. Let $\alpha_1 = g(\alpha_0)$, et cetera and define

$$\alpha = \sup_{n<\omega} \alpha_n.$$

This α is closed under g, and by making α_0 arbitrarily large we can make α as large as we like.

93B. Since M is countable, there are only countably many dense sets (they live in M!), say

$$D_1, D_2, \dots, D_n, \dots \in M.$$

Using Choice, let $p_1 \in D_1$, and then let $p_2 \le p_1$ such that $p_2 \in D_2$ (this is possible since D_2 is dense), and so on. In this way we can inductively exhibit a chain

$$p_1 \ge p_2 \ge p_3 \ge \dots$$

with $p_i \in D_i$ for every i.

Hence, we want to generate a filter from the $\{p_i\}$. Just take the upwards closure – let G be the set of $q \in \mathbb{P}$ such that $q \ge p_n$ for some n. By construction, G is a filter (this is actually trivial). Moreover, G intersects all the dense sets by construction.

94A. It suffices to show that $\mathbb{P}$ preserves regularity greater than or equal to κ. Consider $\lambda > \kappa$ which is regular in M, and suppose for contradiction that λ is not regular in $M[G]$. That's the same as saying that there is a function $f \in M[G]$, $f \colon \overline{\lambda} \to \lambda$ cofinal, with $\overline{\lambda} < \lambda$. Then by the Possible Values Argument, there exists a function $F \in M$ from $\overline{\lambda} \to \mathcal{P}(\lambda)$ such that $f(\alpha) \in F(\alpha)$ and $|F(\alpha)|^M < \kappa$ for every α.

Now we work in M again. Note for each $\alpha \in \overline{\lambda}$, $F(\alpha)$ is bounded in λ since λ is regular in M and greater than $|F(\alpha)|$. Now look at the function $\overline{\lambda} \to \lambda$ in M by just

$$\alpha \mapsto \cup F(\alpha) < \lambda.$$

This is cofinal in M, contradiction.

D Glossary of notations

§D.1 General

- $\forall$: for all
- $\exists$: there exists
- $\operatorname{sign}(\sigma)$: sign of permutation σ
- $X \implies Y$: X implies Y

§D.2 Functions and sets

- $f^{\text{img}}(S)$ is the image of $f\colon X \to Y$ for $S \subseteq X$.
- $f^{-1}(y)$ is the inverse for $f\colon X \to Y$ when $y \in Y$.
- $f^{\text{pre}}(T)$ is the pre-image for $f\colon X \to Y$ when $T \subseteq Y$.
- $f\restriction_S$ is the restriction of $f\colon X \to Y$ to $S \subseteq X$.
- f^n is the function f applied n times

Below are some common sets. These may also be thought of as groups, rings, fields etc. in the obvious way.

- $\mathbb{C}$: set of complex numbers
- $\mathbb{R}$: set of real numbers
- $\mathbb{N}$: set of positive integers
- $\mathbb{Q}$: set of rational numbers
- $\mathbb{Z}$: set of integers
- $\varnothing$: empty set

Some common notation with sets:

- $A \subset B$: A is any subset of B
- $A \subseteq B$: A is any subset of B
- $A \subsetneq B$: A is a *proper* subset of B
- $S \times T$: Cartesian product of sets S and T
- $S \setminus T$: difference of sets S and T
- $S \cup T$: set union of S and T
- $S \cap T$: set intersection of S and T

- $S \sqcup T$: disjoint union of S and T
- $|S|$: cardinality of S
- $S/{\sim}$: if $\sim$ is an equivalence relation on S, this is the set of equivalence classes
- $x+S$: denotes the set $\{x+s \mid s \in S\}$.
- xS: denotes the set $\{xs \mid s \in S\}$.

§D.3 Abstract and linear algebra

Some common groups/rings/fields:

- $\mathbb{Z}/n\mathbb{Z}$: cyclic group of order n
- $(\mathbb{Z}/n\mathbb{Z})^\times$: set of units of $\mathbb{Z}/n\mathbb{Z}$.
- S_n: symmetric group on $\{1,\dots,n\}$
- D_{2n}: dihedral group of order $2n$.
- 0, 1: trivial group (depending on context)
- $\mathbb{F}_p$: integers modulo p

Notation with groups:

- 1_G: identity element of the group G
- $N \trianglelefteq G$: subgroup N is normal in G.
- G/N: quotient group of G by the normal subgroup N
- $Z(G)$: center of group G
- $N_G(H)$: normalizer of the subgroup H of G
- $G \times H$: product group of G and H
- $G \oplus H$: also product group, but often used when G and H are abelian (and hence we can think of them as $\mathbb{Z}$-modules)
- $\operatorname{Stab}_G(x)$: the stabilizer of $x \in X$, if X is acted on by G
- $\operatorname{FixPt} g$, the set of fixed points by $g \in G$ (under a group action)

Notation with rings:

- R/I: quotient of ring R by ideal I
- $(a_1,\dots,a_n)$: ideal generated by the a_i
- $R^\times$: the group of units of R
- $R[x_1,\dots,x_n]$: polynomial ring in x_i, or ring obtained by adjoining the x_i to R
- $F(x_1,\dots,x_n)$: field obtained by adjoining x_i to F
- R^d: dth graded part of a graded (pseudo)ring R

Linear algebra:

- id: the identity matrix
- $V \oplus W$: direct sum
- $V^{\oplus n}$: direct sum of V, n times
- $V \otimes W$: tensor product
- $V^{\otimes n}$: tensor product of V, n times
- $V^\vee$: dual space
- $T^\vee$: dual map (for T a vector space)
- $T^\dagger$: conjugate transpose (for T a vector space)
- $\langle -, - \rangle$: a bilinear form
- $\operatorname{Mat}(V)$: endomorphisms of V, i.e. $\operatorname{Hom}_k(V, V)$
- $\mathbf{e}_1, \dots, \mathbf{e}_n$: the "standard basis" of $k^{\oplus n}$

§D.4 Quantum computation

- $|\psi\rangle$: a vector in some vector space H
- $\langle\psi|$: a vector in some vector space $H^\vee$, dual to $|\psi\rangle$.
- $\langle\phi|\psi\rangle$: evaluation of an element $\langle\phi| \in H^\vee$ at $|\phi\rangle \in H$.
- $|\uparrow\rangle$, $|\downarrow\rangle$: spin z-up, spin z-down
- $|\rightarrow\rangle$, $|\leftarrow\rangle$: spin x-up, spin x-down
- $|\otimes\rangle$, $|\odot\rangle$: spin y-up, spin y-down

§D.5 Topology and real/complex analysis

Common topological spaces:

- S^1: the unit circle
- S^n: surface of an n-sphere (in $\mathbb{R}^{n+1}$)
- D^{n+1}: closed $n+1$ dimensional ball (in $\mathbb{R}^{n+1}$)
- $\mathbb{RP}^n$: real projective n-space
- $\mathbb{CP}^n$: complex projective n-space

Some topological notation:

- ∂Y: boundary of a set Y (in some topological space)
- X/S: quotient topology of X by $S \subseteq X$
- $X \times Y$: product topology of spaces X and Y

- $X \amalg Y$: disjoint union of spaces X and Y
- $X \vee Y$: wedge product of (pointed) spaces X and Y

Real analysis (calculus 101):

- $\liminf$: limit infimum
- $\limsup$: limit supremum
- $\inf$: infimum
- $\sup$: supremum
- $\mathbb{Z}_p$: p-adic integers
- $\mathbb{Q}_p$: p-adic numbers
- f': derivative of f
- $\int_a^b f(x)\,dx$: Riemann integral of f on $[a,b]$

Complex analysis:

- $\int_\alpha f\,dz$: contour integral of f along path α
- $\operatorname{Res}(f;p)$: the residue of a meromorphic function f at point p
- $\mathbf{I}(\gamma,p)$: winding number of γ around p.

§D.6 Measure theory and probability

- $\mathscr{A}^{\text{cm}}$: the σ-algebra of Caratheory-measurable sets
- $\mathscr{B}(X)$: the Borel space for X
- μ^{cm}: the induced measure on $\mathscr{A}^{\text{cm}}$.
- λ: Lebesgue measure
- $\mathbf{1}_A$: the indicator function for A
- $\int_\Omega f\,d\mu$: the Lebesgue integral of f
- $\lim_{n\to\infty} f_n$: pointwise limit of f_n
- $\widehat{G}$: Pontryagin dual for G

§D.7 Algebraic topology

- $\alpha \simeq \beta$: for paths, this indicates path homotopy
- $*$: path concatenation
- $\pi_1(X) = \pi_1(X, x_0)$: the fundamental group of (pointed) space X
- $\pi_n(X) = \pi_n(X, x_0)$: the nth homotopy group of (pointed) space X
- $f_\sharp$: the induced map $\pi_1(X) \to \pi_1(Y)$ of $f \colon X \to Y$

- Δ^n: the standard n-simplex
- $\partial\sigma$: the boundary of a singular n-simplex σ
- $H_n(A_\bullet)$: the nth homology group of the chain complex $A_\bullet$
- $H_n(X)$: the nth homology group of a space X
- $\widetilde{H}_n(X)$: the nth reduced homology group of X
- $H_n(X, A)$: the nth relative homology group of X and $A \subseteq X$
- f_*: the induced map on $H_n(A_\bullet) \to H_n(B_\bullet)$ of $f\colon A_\bullet \to B_\bullet$, or $H_n(X) \to H_n(Y)$ for $f\colon X \to Y$
- $\chi(X)$: Euler characteristic of a space X
- $H^n(A^\bullet)$: the nth cohomology group of a cochain complex $A^\bullet$
- $H^n(A_\bullet; G)$: the nth cohomology group of the cochain complex obtained by applying $\operatorname{Hom}(-, G)$ to $A_\bullet$
- $H^n(X; G)$: the nth cohomology group/ring of X with G-coefficients
- $\widetilde{H}^n(X; G)$: the nth reduced cohomology group/ring of X with G-coefficients
- $H^n(X, A; G)$: the nth relative cohomology group/ring of X and $A \subset X$ with G-coefficients
- $f^\sharp$: the induced map on $H^n(A^\bullet) \to H^n(B^\bullet)$ of $f\colon A^\bullet \to B^\bullet$, or $H^n(X) \to H^n(Y)$ for $f\colon X \to Y$
- $\operatorname{Ext}(-,-)$: the Ext functor
- $\phi \smile \psi$: cup product of cochains ϕ and ψ

§D.8 Category theory

Some common categories (in alphabetical order):

- Grp: category of groups
- CRing: category of commutative rings
- Top: category of topological spaces
- Top_*: category of pointed topological spaces
- Vect_k: category of k-vector spaces
- FDVect_k: category of finite-dimensional vector spaces
- Set: category of sets
- hTop: category of topological spaces, whose morphisms are homotopy classes of maps
- hTop_*: pointed version of hTop

- $\mathsf{hPairTop}$: category of pairs (X, A) with morphisms being pair-homotopy equivalence classes
- $\operatorname{OpenSets}(X)$: the category of open sets of X, as a poset

Operations with categories:

- $\operatorname{obj} \mathcal{A}$: objects of the category $\mathcal{A}$
- $\mathcal{A}^{\text{op}}$: opposite category
- $\mathcal{A} \times \mathcal{B}$: product category
- $[\mathcal{A}, \mathcal{B}]$: category of functors from $\mathcal{A}$ to $\mathcal{B}$
- $\ker f \colon \operatorname{Ker} f \to B$: for $f \colon A \to B$, categorical kernel
- $\operatorname{coker} f \colon A \to \operatorname{Coker} f$: for $f \colon A \to B$, categorical cokernel
- $\operatorname{im} f \colon A \to \operatorname{Im} f$: for $f \colon A \to B$, categorical image

§D.9 Differential geometry

- Df: total derivative of f
- $(Df)_p$: total derivate of f at point p
- $\frac{\partial f}{\partial e_i}$: i^{th} partial derivative
- α_p: evaluating a k-form α at p
- $\int_c \alpha$: integration of the differential form α over a cell c
- $d\alpha$: exterior derivative of a k-form α
- $\phi^* \alpha$: pullback of k-form α by ϕ

§D.10 Algebraic number theory

- $\overline{\mathbb{Q}}$: ring of algebraic numbers
- $\overline{\mathbb{Z}}$: ring of algebraic integers
- $\overline{F}$: algebraic closure of a field F
- $\operatorname{N}_{K/\mathbb{Q}}(\alpha)$: the norm of α in extension $K/\mathbb{Q}$
- $\operatorname{Tr}_{K/\mathbb{Q}}(\alpha)$: the trace of α in extension $K/\mathbb{Q}$
- $\mathcal{O}_K$: ring of integers in K
- $\mathfrak{a} + \mathfrak{b}$: sum of two ideals $\mathfrak{a}$ and $\mathfrak{b}$
- $\mathfrak{a}\mathfrak{b}$: ideal generated by products of elements in ideals $\mathfrak{a}$ and $\mathfrak{b}$
- $\mathfrak{a} \mid \mathfrak{b}$: ideal $\mathfrak{a}$ divides ideal $\mathfrak{b}$
- $\mathfrak{a}^{-1}$: the inverse of $\mathfrak{a}$ in the ideal group

- $\mathrm{N}(I)$: ideal norm
- Cl_K: class group of K
- Δ_K: discriminant of number field K
- $\mu(\mathcal{O}_K)$: set of roots of unity contained in $\mathcal{O}_K$
- $[K : F]$: degree of a field extension
- $\mathrm{Aut}(K/F)$: set of field automorphisms of K fixing F
- $\mathrm{Gal}(K/F)$: Galois group of K/F
- $D_{\mathfrak{p}}$: decomposition group of prime ideal $\mathfrak{p}$
- $I_{\mathfrak{p}}$: inertia group of prime ideal $\mathfrak{p}$
- $\mathrm{Frob}_{\mathfrak{p}}$: Frobenius element of $\mathfrak{p}$ (element of $\mathrm{Gal}(K/\mathbb{Q})$)
- $P_K(\mathfrak{m})$: ray of principal ideals of a modulus $\mathfrak{m}$
- $I_K(\mathfrak{m})$: fractional ideals of a modulus $\mathfrak{m}$
- $C_K(\mathfrak{m})$: ray class group of a modulus $\mathfrak{m}$
- $\left(\frac{L/K}{\bullet}\right)$: the Artin symbol
- $\mathrm{Ram}(L/K)$: primes of K ramifying in L
- $\mathfrak{f}(L/K)$: the conductor of L/K

§D.11 Representation theory

- $k[G]$: group algebra
- $V \oplus W$: direct sum of representations $V = (V, \rho_V)$ and $W = (W, \rho_W)$ of an algebra A
- $V^\vee$: dual representation of a representation $V = (V, \rho_V)$
- $\mathrm{Reg}(A)$: regular representation of an algebra A
- $\mathrm{Hom}_{\mathrm{rep}}(V, W)$: algebra of morphisms $V \to W$ of representations
- χ_V: the character $A \to k$ attached to an A-representation V
- $\mathrm{Classes}(G)$: set of conjugacy classes of G
- $\mathrm{Fun}_{\mathrm{class}}(G)$: the complex vector space of functions $\mathrm{Classes}(G) \to \mathbb{C}$
- $V \otimes W$: tensor product of representations $V = (V, \rho_V)$ and $W = (W, \rho_W)$ of a *group* G (rather than an algebra)
- $\mathbb{C}_{\mathrm{triv}}$: the trivial representation
- $\mathbb{C}_{\mathrm{sign}}$: the sign representation

§D.12 Algebraic geometry

- $\mathcal{V}(-)$: vanishing locus of a set or ideal
- $\mathbb{A}^n$: n-dimensional (complex) affine space
- $\sqrt{I}$: radical of an ideal I
- $\mathbb{C}[V]$: coordinate ring of an affine variety V
- $\mathcal{O}_V(U)$: ring of rational functions on U
- $D(f)$: distinguished open set
- $\mathbb{CP}^n$: complex projective n-space (ambient space for projective varieties)
- $(x_0 : \dots : x_n)$: coordinates of projective space
- U_i: standard affine charts
- $\mathcal{V}_{\text{pr}}(-)$: projective vanishing locus.
- h_I, h_V: Hilbert function of an ideal I or projective variety V
- $\pi^\sharp$ or $\pi^\sharp_U$: the pullback $\mathcal{O}_Y \to \mathcal{O}_X(\pi^{\text{pre}}(U))$ obtained from $\pi\colon X \to Y$
- $\mathscr{F}_p$: the stalk of a (pre-)sheaf $\mathscr{F}$ at a point p
- $[s]_p$: the germ of $s \in \mathscr{F}(U)$ at the point p
- $\mathcal{O}_{X,p}$: shorthand for $(\mathcal{O}_X)_p$.
- $\mathscr{F}^{\text{sh}}$: sheafification of pre-sheaf $\mathscr{F}$
- $\alpha_p\colon \mathscr{F}_p \to \mathscr{G}_p$: morphism of stalks obtained from $\alpha\colon \mathscr{F} \to \mathscr{G}$
- $\mathfrak{m}_{X,p}$: the maximal ideal of $\mathcal{O}_{X,p}$
- $\operatorname{Spec} A$: the spectrum of a ring A
- $S^{-1}A$: localization of ring A at a set S
- $A[1/f]$: localization of ring A away from element f
- $A_\mathfrak{p}$: localization of ring A at prime ideal $\mathfrak{p}$
- $f(\mathfrak{p})$: the value of f at $\mathfrak{p}$, i.e. $f \pmod{\mathfrak{p}}$
- $\kappa(\mathfrak{p})$: the residue field of $\operatorname{Spec} A$ at the element $\mathfrak{p}$.
- $\pi^\sharp_\mathfrak{p}$: the induced map of stalks in $\pi^\sharp$.

§D.13 Set theory

- ZFC: standard theory of ZFC
- ZFC$^+$: standard theory of ZFC, plus the sentence "there exists a strongly inaccessible cardinal"
- 2^S or $\mathcal{P}(S)$: power set of S
- $A \wedge B$: A and B
- $A \vee B$: A or B
- $\neg A$: not A
- V: class of all sets (von Neumann universe)
- ω: the first infinite ordinal, also the set of nonnegative integers
- V_α: level of the von Neumann universe
- On: class of ordinals
- $\bigcup A$: the union of elements inside A
- $A \approx B$: sets A and B are equinumerous
- $\aleph_\alpha$: the aleph numbers
- $\operatorname{cof} \lambda$: the cofinality of λ
- $\mathscr{M} \vDash \phi[b_1, \dots, b_n]$: model $\mathscr{M}$ satisfies sentence ϕ with parameters b_1, …, b_n
- Δ_n, Σ_n, Π_n: levels of the Levy hierarchy
- $\mathscr{M}_1 \subseteq \mathscr{M}_2$: $\mathscr{M}_1$ is a substructure of $\mathscr{M}_2$
- $\mathscr{M}_1 \prec \mathscr{M}_2$: $\mathscr{M}_1$ is an elementary substructure of $\mathscr{M}_2$
- $p \parallel q$: elements p and q of a poset $\mathbb{P}$ are compatible
- $p \perp q$: elements p and q of a poset $\mathbb{P}$ are incompatible
- Name_α: the hierarchy of $\mathbb{P}$-names
- τ^G: interpretation of a name τ by filter G
- $M[G]$: the model obtained from a forcing poset $G \subseteq \mathbb{P}$
- $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$: $p \in \mathbb{P}$ forces the sentence φ
- $\check{x}$: the name giving an $x \in M$ when interpreted
- $\dot{G}$: the name giving G when interpreted

E Terminology on sets and functions

This appendix will cover some notions on sets and functions such as "bijections", "equivalence classes", and so on.

Remark for experts: I am not dealing with foundational issues in this chapter. See Chapter 89 (and onwards) if that's what you're interested in. Consequently I will not prove most assertions.

§E.1 Sets

A **set** for us will just be a collection of elements (whatever they may be). For example, the set $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ is the positive integers, and $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ is the set of all integers. As another example, we have a set of humans:

$$H = \{x \mid x \text{ is a featherless biped}\}.$$

(Here the "|" means "such that".)

There's also a set with no elements, which we call the **empty set**. It's denoted by $\varnothing$.

It's conventional to use capital letters for sets (like H), and lowercase letters for elements of sets (like x).

Definition E.1.1. We write $x \in S$ to mean "x is in S", for example $3 \in \mathbb{N}$.

Definition E.1.2. If every element of a set A is also in a set B, then we say A is a **subset** of B, and denote this by $A \subseteq B$. If moreover $A \neq B$, we say A is a **proper subset** and write $A \subsetneq B$. (This is analogous to $\le$ and $<$.)

Given a set A, the set of all subsets is denoted 2^A or $\mathcal{P}(A)$ and called the **power set** of A.

Example E.1.3 (Examples of subsets)

(a) $\{1, 2, 3\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$.

(b) $\varnothing \subseteq A$ for any set A. (Why?)

(c) $A \subseteq A$ for any set A.

(d) If $A = \{1, 2\}$ then $2^A = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$.

Definition E.1.4. We write

- $A \cup B$ for the set of elements in *either* A or B (possibly both), called the **union** of A and B.
- $A \cap B$ for the set of elements in *both* A and B, and called the **intersection** of A and B.
- $A \setminus B$ for the set of elements in A but *not* in B.

Example E.1.5 (Examples of set operations)
Let $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$. Then

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4, 5\} \\ A \cap B &= \{3\} \\ A \setminus B &= \{1, 2\}. \end{aligned}$$

Exercise E.1.6. Convince yourself: for any sets A and B, we have $A \cap B \subseteq A \subseteq A \cup B$.

Here are some commonly recurring sets:

- $\mathbb{C}$ is the set of complex numbers, like $3.2 + \sqrt{2}i$.
- $\mathbb{R}$ is the set of real numbers, like $\sqrt{2}$ or π.
- $\mathbb{N}$ is the set of positive integers, like 5 or 9.
- $\mathbb{Q}$ is the set of rational numbers, like $7/3$.
- $\mathbb{Z}$ is the set of integers, like -2 or 8.

(These are pronounced in the way you would expect: “see”, “are”, “en”, “cue”, “zed”.)

§E.2 Functions

Given two sets A and B, a **function** f from A to B is a mapping of every element of A to some element of B.

We call A the **domain** of f, and B the **codomain**. We write this as $f \colon A \to B$ or $A \xrightarrow{f} B$.

Abuse of Notation E.2.1. If the name f is not important, we will often just write $A \to B$.

We write $f(a) = b$ or $a \mapsto b$ to signal that f takes a to b.

If B has 0 as an element and $f(a) = 0$, we often say a is a **root** or **zero** of f, and that f **vanishes** at a.

§E.2.i Injective / surjective / bijective functions

Definition E.2.2. A function $f \colon A \to B$ is **injective** if it is “one-to-one” in the following sense: if $f(a) = f(a')$ then $a = a'$. In other words, for any $b \in B$, there is *at most* one $a \in A$ such that $f(a) = b$.

Often, we will write $f \colon A \hookrightarrow B$ to emphasize this.

Definition E.2.3. A function $f \colon A \to B$ is **surjective** if it is “onto” in the following sense: for any $b \in B$ there is *at least* one $a \in A$ such that $f(a) = b$.

Often, we will write $f \colon A \twoheadrightarrow B$ to emphasize this.

Definition E.2.4. A function $f \colon A \to B$ is **bijective** if it is both injective and surjective. In other words, for each $b \in B$, there is *exactly* one $a \in A$ such that $f(a) = b$.

Example E.2.5 (Examples of functions)

By “human” I mean “living featherless biped”.

(a) There’s a function taking every human to their age in years (rounded to the nearest integer). This function is **not injective**, because for example there are many people with age 20. This function is also **not surjective**: no one has age 10000.

(b) There’s a function taking every USA citizen to their social security number. This is also **not surjective** (no one has SSN equal to 3), but at least it **is injective** (no two people have the same SSN).

Example E.2.6 (Examples of bijections)

(a) Let $A = \{1,2,3,4,5\}$ and $B = \{6,7,8,9,10\}$. Then the function $f\colon A \to B$ by $a \mapsto a+5$ is a bijection.

(b) In a classroom with 30 seats, there is exactly one student in every seat. Thus the function taking each student to the seat they’re in is a bijection; in particular, there are exactly 30 students.

Remark E.2.7 — Assume for convenience that A and B are finite sets. Then:

- If $f\colon A \hookrightarrow B$ is injective, then the size of A is at most the size of B.
- If $f\colon A \twoheadrightarrow B$ is surjective, then the size of A is at least the size of B.
- If $f\colon A \to B$ is a bijection, then the size of A equals the size of B.

Now, notice that if $f\colon A \to B$ is a bijection, then we can “apply f backwards”: (for example, rather than mapping each student to the seat they’re in, we map each seat to the student sitting in it). This is called an **inverse function**; we denote it $f^{-1}\colon B \to A$.

§E.2.ii Images and pre-images

Let $X \xrightarrow{f} Y$ be a function.

Definition E.2.8. Suppose $T \subseteq Y$. The **pre-image** $f^{\text{pre}}(T)$ is the set of all $x \in X$ such that $f(x) \in T$. Thus, $f^{\text{pre}}(T)$ is a subset of X.

Example E.2.9 (Examples of pre-image)

Let $f\colon H \to \mathbb{Z}$ be the age function from earlier. Then

(a) $f^{\text{pre}}(\{13,14,15,16,17,18,19\})$ is the set of teenagers.

(b) $f^{\text{pre}}(\{0\})$ is the set of newborns.

(c) $f^{\text{pre}}(\{1000,1001,1002,\dots\}) = \varnothing$, as I don’t think anyone is that old.

Abuse of Notation E.2.10. By abuse of notation, we may abbreviate $f^{\text{pre}}(\{y\})$ to $f^{\text{pre}}(y)$. So for example, $f^{\text{pre}}(\{0\})$ above becomes shortened to $f^{\text{pre}}(0)$.

The dual notion is:

Definition E.2.11. Suppose $S \subseteq X$. The **image** $f^{\text{img}}(S)$ is the set of all things of the form $f(s)$.

Example E.2.12 (Examples of images)

Let $A = \{1, 2, 3, 4, 5\}$ and $B = \mathbb{Z}$. Consider a function $f \colon A \to B$ given by

$$f(1) = 17 \quad f(2) = 17 \quad f(3) = 19 \quad f(4) = 30 \quad f(5) = 234.$$

(a) The image $f^{\text{img}}(\{1, 2, 3\})$ is the set $\{17, 19\}$.

(b) The image $f^{\text{img}}(A)$ is the set $\{17, 19, 30, 234\}$.

Question E.2.13. Suppose $f \colon A \twoheadrightarrow B$ is surjective. What is $f^{\text{img}}(A)$?

§E.3 Equivalence relations

Let X be a fixed set now. A binary relation $\sim$ on X assigns a truth value "true" or "false" to $x \sim y$ for each x or y. Now an **equivalence relation** $\sim$ on X is a binary relation which satisfies the following axioms:

- Reflexive: we have $x \sim x$.
- Symmetric: if $x \sim y$ then $y \sim x$
- Transitive: if $x \sim y$ and $y \sim z$ then $x \sim z$.

An **equivalence class** is then a set of all things equivalent to each other. One can show that X becomes partitioned by these equivalence classes:

Example E.3.1 (Example of an equivalence relation)

Let $\mathbb{N}$ denote the set of positive integers. Then suppose we declare $a \sim b$ if a and b have the same last digit, for example $131 \sim 211$, $45 \sim 125$, and so on.

Then $\sim$ is an equivalence relation. It partitions $\mathbb{N}$ into ten equivalence classes, one for each trailing digit.

Often, the set of equivalence classes will be denoted $X/{\sim}$ (pronounced "X mod sim").

Image Attributions

[1207] 127“RECT”. *Cantor set in seven iterations.* Public domain. 2007. URL: https://en.wikipedia.org/wiki/File:Cantor_set_in_seven_iterations.svg (cited p. 394)

[ca] POP-UP CASKET. *Omega exp.* Public domain. URL: https://commons.wikimedia.org/wiki/File:Omega-exp-omega-labeled.svg (cited p. 911)

[Ee] EEYORE22. *Weierstrass function.* Public domain. URL: https://commons.wikimedia.org/wiki/File:WeierstrassFunction.svg (cited p. 346)

[Fr] FROPUFF. *Klein bottle.* Public domain. URL: https://en.wikipedia.org/wiki/File:KleinBottle-01.png (cited p. 650)

[Ge] TOPOLOGICAL GIRL’S GENERATION. *Topological Girl’s Generation.* URL: https://topologicalgirlsgeneration.tumblr.com/ (cited p. 53)

[gk] G.KOV. *Normal surface vector.* URL: https://tex.stackexchange.com/a/235142/76888 (cited p. 448)

[Go08] ABSTRUSE GOOSE. *Math Text.* CC 3.0. 2008. URL: https://abstrusegoose.com/12 (cited p. x)

[Go09] ABSTRUSE GOOSE. *Zornaholic.* CC 3.0. 2009. URL: https://abstrusegoose.com/133 (cited p. 914)

[Ho] GEORGE HODAN. *Apple.* Public domain. URL: https://www.publicdomainpictures.net/view-image.php?image=20117 (cited p. 925)

[In] INDUCTIVELOAD. *Klein Bottle Folding.* Public domain. URL: https://commons.wikimedia.org/wiki/File:Klein_Bottle_Folding_1.svg (cited p. 650)

[Kr] PETR KRATOCHVIL. *Velociraptor.* Public domain. URL: https://www.publicdomainpictures.net/view-image.php?image=93881 (cited p. 925)

[Ma12] MATHMATHSMATHEMATICS. *How to Multiply Matrices - A 2x2 Matrix by various sizes.* May 2012. URL: https://youtu.be/pJwslaulUMU (cited p. 147)

[Mu] RANDALL MUNROE. *Rolle’s theorem.* CC 2.5. URL: https://xkcd.com/2042/ (cited p. 322)

[Na] KRISH NAVEDALA. *Stokes patch.* Public domain. URL: https://en.wikipedia.org/wiki/File:Stokes_patch.svg (cited p. 458)

[Or] BEN ORLIN. *The Math Major Who Never Reads Math.* URL: https://mathwithbaddrawings.com/2015/03/17/the-math-major-who-never-reads-math/ (cited p. xi)

[To] TOAHIGHERLEVEL. *Projection color torus.* Public domain. URL: https://en.wikipedia.org/wiki/File:Projection_color_torus.jpg (cited p. 648)

[Wa] BILL WATTERSON. *Calvin and Hobbes.* I think this is fair use. (cited p. 865)

[Wo] WORDSLAUGH. *Covering space diagram.* CC 3.0. URL: https://commons.wikimedia.org/wiki/File:Covering_space_diagram.svg (cited p. 667)

Bibliography

[Ax97] Sheldon Axler. *Linear algebra done right*. New York: Springer, 1997. isbn: 978-0-387-98258-8 (cited pp. 157, 977)

[Ba10] Joseph Bak. *Complex analysis*. New York: Springer Science+Business Media, LLC, 2010. isbn: 978-1-4419-7287-3 (cited p. 345)

[Ch08] Steve Cheng. "A Crash Course on the Lebesgue Integral and Measure Theory". Apr. 2008. url: https://www.gold-saucer.org/math/lebesgue/lebesgue-new.pdf (cited p. 978)

[Et11] Pavel Etingof. "Introduction to Representation Theory". 2011. url: https://math.mit.edu/~etingof/replect.pdf (cited pp. vii, 979)

[Ga03] Andreas Gathmann. "Algebraic Geometry". 2003. url: https://www.mathematik.uni-kl.de/~gathmann/de/alggeom.php (cited pp. vii, 906, 979)

[Ga14] Dennis Gaitsgory. "Math 55a: Honors Abstract and Linear Algebra". 2014. url: https://web.evanchen.cc/coursework.html (cited pp. vii, 977)

[Ga15] Dennis Gaitsgory. "Math 55b: Honors Real and Complex Analysis". 2015. url: https://web.evanchen.cc/coursework.html (cited pp. 335, 977)

[Go11] Timothy Gowers. "Normal subgroups and quotient groups". 2011. url: https://gowers.wordpress.com/2011/11/20/normal-subgroups-and-quotient-groups/ (cited pp. 72, 977)

[Go18] Vadim Gorin. "18.175: Theory of Probability". 2018. url: https://web.archive.org/web/20190617235844/http://web.mit.edu/txz/www/links.html (cited pp. vii, 978)

[Ha02] Allen Hatcher. *Algebraic topology*. Cambridge, New York: Cambridge University Press, 2002. isbn: 0-521-79160-X. url: https://opac.inria.fr/record=b1122188 (cited pp. 647, 733, 744, 754, 761, 773, 778, 783, 979)

[Hi13] A. J. Hildebrand. "Introduction to Analytic Number Theory". 2013. url: https://web.archive.org/web/20230326025121/https://faculty.math.illinois.edu/~hildebr/ant/main.pdf (cited p. 980)

[Ko14] Peter Koellner. "Math 145a: Set Theory I". 2014. url: https://web.evanchen.cc/coursework.html (cited pp. vii, 979)

[Le] Holden Lee. "Number Theory". url: https://github.com/holdenlee/number-theory (cited p. 620)

[Le02] Hendrik Lenstra. "The Chebotarev Density Theorem". 2002. url: https://websites.math.leidenuniv.nl/algebra/ (cited pp. 625, 979)

[Le14] Tom Leinster. *Basic category theory*. Cambridge: Cambridge University Press, 2014. isbn: 978-1-107-04424-1. url: https://arxiv.org/abs/1612.09375 (cited pp. vii, 679, 682, 700, 703, 917, 978)

[Ll15] Seth Lloyd. "18.435J: Quantum Computation". 2015. url: https://web.evanchen.cc/coursework.html (cited pp. vii, 978)

[Ma13a] Laurentiu Maxim. "Math 752 Topology Lecture Notes". 2013. url: https://www.math.wisc.edu/~maxim/752notes.pdf (cited pp. 773, 979, 1013)

[**Ma13**b] Maxima. “Burnside’s Lemma, post 6”. 2013. url: https://www.aops.com/Forum/viewtopic.php?p=3089768#p3089768 (cited p. 212)

[**Mi14**] Alexandre Miquel. “An Axiomatic Presentation of the Method of Forcing”. 2014. url: https://www.fing.edu.uy/~amiquel/forcing/ (cited p. 979)

[**Mi95**] R. Miranda. *Algebraic Curves and Riemann Surfaces*. Dimacs Series in Discrete Mathematics and Theoretical Comput. American Mathematical Society, 1995. isbn: 9780-8218-0268-7 (cited pp. 494, 524, 980)

[**Mu00**] James Munkres. *Topology*. 2nd. Prentice-Hall, Inc., Jan. 2000. isbn: 97881-203-2046-8. url: https://amazon.com/o/ASIN/8120320468/ (cited p. 979)

[**Og10**] Frederique Oggier. “Algebraic Number Theory”. 2010. url: https://feog.github.io/ANT10.pdf (cited pp. 533, 979)

[**Pu02**] C. C. Pugh. *Real mathematical analysis*. New York: Springer, 2002. isbn: 978-0-387-95297-0 (cited pp. vii, 107, 121, 294, 302, 346, 448, 453, 977, 978)

[**Sc07**] W. H. Schikhof. *Ultrametric Calculus: An Introduction to P-Adic Analysis*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2007. isbn: 9780-521-03287-2. url: https://books.google.com/books?id=cBT05R7TH1QC (cited pp. 311, 312)

[**Sj05**] Reyer Sjamaar. “Manifolds and Differential Forms”. 2005. url: https://pi.math.cornell.edu/~sjamaar/manifolds/manifold.pdf (cited pp. vii, 482, 484, 977)

[**Ul08**] Brooke Ullery. “Minkowski Theory and the Class Number”. 2008. url: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Ullery.pdf (cited p. 551)

[**Va17**] Ravi Vakil. “The Rising Sea: Foundations of Algebraic Geometry”. Nov. 2017. url: https://math.stanford.edu/~vakil/216blog/ (cited pp. iii, vii, 799, 800, 806, 807, 873, 885, 906, 979, 980)

[**Ya12**] Andrew Yang. “Math 43: Complex Analysis”. 2012. url: https://math.dartmouth.edu/~m43s12/syllabus.html (cited pp. 345, 351, 978)